LEX LOCALIS

The Role of Cybersecurity in the Public Sphere - The European Dimension

Editors:
Katarzyna Chałubińska-Jentkiewicz
Istvan Hoffman


§
LEX
LOCALIS

Title: The Role of Cybersecurity in the Public Sphere - The European Dimension

Editors: assoc. prof. Katarzyna Chałubińska-Jentkiewicz, Ph.D. (War Studies University in Warsaw, Law Institute; Academic Centre for Cybersecurity Policy), prof. dr. hab., István Hoffman, Ph.D. (Eötvös Loránd University, Faculty of Law; Marie Curie-Skłodowska University, Faculty of Law and Administration; Centre for Social Sciences (Budapest), Institute for Legal Studies)

Reviewer: András Bencsik, Ph.D. (Eötvös Loránd University, Faculty of Law; Károli University, Faculty of Law), assoc. prof. Piotr Milik, Ph.D. (War Studies University in Warsaw, Law Institute)

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 121254659
ISBN 978-961-7124-11-8 (PDF)

First published in 2022 by
Institute for Local Self-Government Maribor
Smetanova ulica 30, 2000 Maribor, Slovenia
www.lex-localis.press, info@lex-localis.press

For Publisher:
assoc. prof. dr. Boštjan Brezovnik, director

Price: free copy

Acknowledgement:
The monograph has been prepared as a result of the research project "The Place of Cybersecurity in the Public Realm. The European Dimension" supported by the Institute for Local Self-Government Maribor, Slovenia.

https://doi.org/10.4335/2022.2 ISBN 978-961-7124-11-8 (PDF)

Available online at http://www.lex-localis.press.

The Role of Cybersecurity in the Public Sphere - The European Dimension

Editors:
Katarzyna Chałubińska-Jentkiewicz
Istvan Hoffman

Maribor, 2022

The Role of Cybersecurity in the Public Sphere - The European Dimension

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ & ISTVAN HOFFMAN

Abstract The aim of this paper is to present the areas in EU and domestic legal systems which cover currently applicable laws on cybersecurity and the related cyber-liability. Legal regulations related to cybersecurity that are currently in force embrace only a very narrow understanding of the notions of cyberspace and cybercrime. This paper aims to present those areas of the existing regulations in which the notions of cyber-liability have been preliminarily defined. Issues that are currently viewed as only marginally relevant to the functioning of states in the domain of cyberspace operations or artificial intelligence are also related to cyber-liability. The paper covers issues related to online platforms as well as the role of the state and public administration, network technologies and financial institutions in cybersecurity system especially from European perspective. It also investigates the issues related to strategic and political responsibility, cooperation mechanisms, obligations of telecommunication entrepreneurs, personal data and drone operations in public space. Part of the paper is also related to the movement of cultural assents, digital platforms, blocking injunctions and blocking access, threats of the cyberterrorism, cybersecurity, cybercrime in Hungary, including COVID-19 environment, as well as authorities competent for cybersecurity in Germany. This broad perspective is used to better understand regulatory purposes in European contexts to secure digital society development.

Keywords: • cybersecurity • cyberattack • cyberthreat • cybercrime • cyberspace • digitalization • network technologies

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Associate Professor, War Studies University in Warsaw, Law Institute, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland; Head of the Academic Centre for Cybersecurity Policy, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: kasiachalubinska@gmail.com. István Hoffman, Ph.D., Prof. Dr. Hab., Eötvös Loránd University, Faculty of Law, Department of Administrative Law, 1053 Budapest, Egyetem tér 1-3, Hungary, e-mail: hoffman.istvan@ajk.elte.hu; Marie Curie-Skłodowska University, Faculty of Law and Administration, Department of International Public Law, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland, e-mail: i.hoffman@poczta.umcs.lublin.pl; Senior Research Fellow, Centre for Social Sciences, Institute for Legal Studies, 1097 Budapest, Tóth Kálmán u. 2-4, Hungary, e-mail: hoffman.istvan@tk.mta.hu.

https://doi.org/10.4335/2022.2 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

Table of Content

Introduction

Despite all disappointments, failures and tragic mistakes, people will build a better world. If they were not to act with that thought, we would lose all faith in humanity and its potential, in which case it would be better not to live at all, my friends.
Stanisław Lem, Dialogues [1]

An area that has been partially regulated by law, and one that has special prominence in legal systems, is cybersecurity. Cybersecurity needs to be considered as an interdisciplinary concept that draws on multiple fields (including various sub-fields of law). However, in order to distinguish them from the legal and administrative system as a whole (in relation to the latter, especially in organisational and subjective terms), and to categorise it and identify regulatory areas, it is necessary to define the scope of activity that this sphere involves (in subjective, objective, functional and organisational terms). Only then will it be possible to systematise the issues of the legal protection of cyberspace. And this is the aim of this preliminary study addressing the fundamental issues related to the shared responsibility of individuals and the state in cyberspace.

Under current legal circumstances, the approach taken by regulatory bodies to the issue of cybersecurity results from cybersecurity being associated with the need to counter attacks primarily targeting ICT networks. However, such a standpoint seems groundless, especially in the context of the concept of cyberspace and threats related to it. For the purposes of this study, cybersecurity is assumed to refer to ensuring the protection of, and countering threats that affect, cyberspace, as well as functioning in cyberspace, and this concerns both public and private sectors and their interrelations. This view is supported by the characteristics of cybercrime, which generally encompasses threats emerging in cyberspace (Chałubińska-Jentkiewicz, 2019: 8).

When addressing issues related to cybersecurity and the threats associated with it, including cybercrime and cyber-liability, it is important to consider separately the following questions: Generally speaking, what is cyberspace and how are we responsible for any actions within it? What legal regulations have been adopted so far within national and international law? How are these enforced and is it correct for these to be based on the regulations that apply to the non-virtual realm? What is cybercrime? What are the powers of the organisations responsible for fighting cybercrime and, by extension, what are the rights and responsibilities of actors operating in cyberspace? Are internet users responsible for their online actions? Are they responsible jointly and severally with service providers? How should we balance individual interests, including the right to privacy, and public interest, which involves actions related to defining liability for online actions? The backdrop for these problems are issues such as current strategic and

[1] Dialogues, Wydawnictwo Literackie, Kraków – Wrocław 1984, p. 287.

regulatory policies for cyberspace, and the related security challenges and legal regulations to ensure a secure cyberspace.

The aim of this paper is to present the areas in EU and domestic legal systems which cover currently applicable laws on cybersecurity and the related cyber-liability. In order to investigate this subject matter, it is necessary to:

- establish a detailed definition, and the subjective and objective scope of, cybersecurity, and its classification within the overall security domain;
- review domestic regulations on cybersecurity and cyber-liability in the digital era;
- analyse and assess the applicable laws on cyber-liability, taking into consideration the constitutionally permissible restrictions in the area of individual rights and freedoms;
- analyse and assess legal solutions related to cybersecurity applicable to electronic communications (telecom regulations, taking into account the legal regulations concerning activities in ICT networks – the Act on Providing Services by Electronic Means, and the law regulating new technologies and the functioning of networks and computers).

It is worth stressing that the legal regulations related to cybersecurity that are currently in force embrace only a very narrow understanding of the notions of cyberspace and cybercrime. This paper aims to present those areas of the existing regulations in which the notions of cyber-liability have been preliminarily defined. However, all the issues that are currently viewed as only marginally relevant to the functioning of states in the domain of cyberspace operations or artificial intelligence are also related to cyber-liability. The latter issues go well beyond the contemporary regulatory directions applicable to cyberspace, whereas we mistakenly take the standpoint that real-world regulation is to be reflected in cybersecurity-related regulation.

References:

Chałubińska – Jentkiewicz, K. (2019) Cyberbezpieczeństwo – zagadnienia definicyjne, *Cybersecurity & Law*, 2(2), pp. 7-25.

Online Platforms in the Cybersecurity System

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Abstract The issue of cyberspace security is determined by the development of new technologies, including robotics and digital processes, and the state's computerisation progress. The fundamental issue of legal protection in the cybersecurity system is to determine the subjective and objective scope of responsibility for online activities. One of the key regulations regarding liability in the field of cybersecurity is the NIS Directive and its draft amendment, the so-called NIS 2. Technological change in the field of communication has fundamentally modified the ways individuals and entire communities function. It should be ensured that hosting service providers process the received counter-notices in the proper manner. As a result of technological and economic convergence, the same entity may perform very different functions, and it is not determined what its status will be, so the scope of its liability is not conclusively determined. The situation calls for appropriate regulations, with the reservation that there is a need to synchronise issues at each stage of legislative activity.

Keywords: • cybersecurity • cyberspace • online platforms • digital services • e-services • digital content • responsibility • liability • digital infrastructure

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Associate Professor, War Studies University in Warsaw, Law Institute, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland; Head of the Academic Centre for Cybersecurity Policy, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: kasiachalubinska@gmail.com.

https://doi.org/10.4335/2022.2.1 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Duties and responsibilities

The notion of network security or cybersecurity covers, *inter alia*, the protection of resources – data, information and, more generally, digital content, the protection of ICT networks and devices, i.e., computers, and also the protection of content transmission via networks, so the communication process itself. The human factor is also worth noting here, namely the protection of network and computer users. It should definitely be stressed that human activity is still an important element in the process, and this is perhaps one of the underlying dilemmas regarding the future of cybersecurity.

The issue of cyberspace security is determined by the development of new technologies, including robotics and digital processes, and the state's computerisation progress. The latter is a key element for the development of cybersecurity administration which can be perceived from two different angles. The first may refer to cybersecurity administration in the objective sense, concerning a specific group of institutions with certain competences and tasks, while the second is connected with positive law applied with a view to implementing the state's cybersecurity mission, goals and tasks, both nationally or internationally. It is worth stressing that legal provisions which can be nowadays classified as those regulating the issue of cybersecurity are very often dispersed and cover different areas of human life. The issue of such dispersion was not successfully resolved by the National Cybersecurity System Act of 5 July 2018 (Journal of Laws of 2018, item 1560) (hereinafter: the National System Act) implementing the NIS Directive into Polish legislation. Nonetheless, it should be emphasised that the fundamental issue of legal protection in the cybersecurity system is to determine the subjective and objective scope of responsibility for online activities. First and foremost, however, it is necessary to define what digital content is and when it can be deemed illegal, as well as to answer the question of who bears liability for it and to what extent.

2 Duties of digital providers in light of the NIS Directive and the National Cybersecurity System Act

One of the key regulations regarding liability in the field of cybersecurity is the NIS Directive and its draft amendment, the so-called NIS 2, which is meant to replace the original act, so as "to address the increased interconnectedness between the physical and digital world through a legislative framework with robust resilience measures, both for cyber and physical aspects as set out in the EU Security Union Strategy" (COM(2020) 605). The amendment is aimed at increasing the resilience of "essential actors" and "relevant actors" reaching certain thresholds in numerous sectors against all threats connected with information and communication technologies (ICTs). The opportunities offered by new technologies and the need to properly adjust the administrative and legal system are crucial issues for the development of modern ICT network security management. Public authorities are now obliged to provide electronic services to citizens, covering both citizen services and other areas of public administration, not excluding the decision-making process. The impact of new technical means which were introduced into

public administration forces some changes in basic administrative and legal relations (individual-citizen), and is of great significance for the inter-sector cooperation in the course of the implementation of public tasks. Cyberspace is a new domain of impact exerted by these processes. Along with the development of cyberspace, the threats which are connected with it also evolve. Currently, cyberspace is a symbol of development, but also of freedom and privacy, and any interference in its functioning tends to be viewed as an attack on these values. However, in the states engaged in building an information society, cybersecurity is considered one of the most serious challenges for the national security system. It refers to the security of both the entire state institution and individual citizens. The responsibility for ensuring cybersecurity applies to all network users, but a significant role is played by public administration bodies whose basic tasks include taking measures to ensure security and public order. As part of arranging for the implementation of public tasks oriented towards ensuring national security, with particular emphasis on the definition of public tasks in the field of critical infrastructure protection, it is important to establish a list of entities carrying out public tasks in the field of cybersecurity. It should be remarked that these entities may include public entities performing public tasks, private entities performing public tasks due to the privatisation of public task performance, and private entities performing their own tasks which are of particular importance for the public interest, or which were once performed as public tasks but were then subject to privatisation. In consequence, the issue of inter-sector cooperation becomes significant in the process of establishing a unified cybersecurity system. This platform has given rise to certain measures and more intensive cooperation between the public and private sectors as regards the identification of key resources, means, functions and underlying requirements for resilience, as well as the need for cooperation and mechanisms to respond to large-scale disruptions of electronic communications. For this reason, digital service providers are becoming a major element of the EU cybersecurity system.

Digital service providers are legal persons or organisational units without legal personality having their registered office or management board in the territory of the Republic of Poland, or acting via a representative having its organisational unit in the territory of the Republic of Poland, providing digital services, including services rendered by electronic means, within the meaning of the Act on the Provision of Services by Electronic Means. Legal commentators separately distinguish entities providing digital services. J. Barta and R. Markiewicz distinguish the following categories of entities: telecommunication network holders/operators – telecommunication companies; access providers – entities providing services which consist in enabling access to the network without any influence on the content transmitted through that network; primary network content providers, content providers – entities whose activity consists in introducing their "own" content into the network, which allows other users to use this material; and network service providers (service providers) (Barta, 2014:213-215). (More information in Gęsicka 2014:40-49). M. Zieliński distinguishes three categories of entities falling within the service provider category, i.e., access providers, network providers and intermediary service providers. He also mentions content providers (Zieliński: 2013:38).

A similar distinction is applied by Litwiński (2004:176-178). The legislator excluded from the application of the Act those entrepreneurs (micro- and small entrepreneurs) who are referred to in Article 7(1)(1) and (2) of the Act of 6 March 2018 – Entrepreneurs Law (Journal of Laws of 2021, item 162, 2105).

The notion of e-service, which is given a similar meaning to that attributable to the notion of information society services in Directive 2000/31/EC, is related to the concept of digital services, including those provided by electronic means. This service was defined as a service provided in an automated manner through the use of information technology, by means of ICT systems on public telecommunications networks, at the individual request of the service recipient, without the simultaneous presence of the parties in the same location; however, e-services do not include: a) radio and television broadcasting services, b) telecommunications services, c) the supply of the following goods and services: goods in the case of which the ordering and order processing is done electronically, CD-ROMs, floppy disks and similar physical media, printed material such as books, bulletins, newspapers and magazines, CDs, cassettes, video tapes, DVDs, games on CD-ROM, services provided by lawyers or financial advisers who offer advice by e-mail, educational services during which the course content is delivered by the instructor via the internet or an electronic network (i.e., remotely), off-line physical repair services of computer equipment, off-line data warehousing, advertising services, in particular in newspapers, on posters and on television, call centres, educational services provided by correspondence, especially through the post, conventional auction house services involving human intervention, irrespective of the bid submission mode, telephone services with a video component, access to the internet and websites, and telephone services provided via the internet. In the Regulation of the Minister of Regional Development of 21 March 2013 on granting financial aid by the Polish Agency for Enterprise Development to support the establishing and development of electronic economy under the Operational Programme Innovative Economy 2007-2013, e-service was defined as a service provided in an automated manner, with the use of information technology, by means of ICT systems in public telecommunications networks, at the individual request of a recipient of services, without the simultaneous presence of the parties in the same location; however, e-services do not include: a) radio and television broadcasting services, b) telecommunication services, c) the supply of the following goods and services: – goods in the case of which the ordering and order processing is done electronically, – mobile computer storage media, – printed material such as books, bulletins, newspapers and magazines, – sound recordings on analogue or computer storage media, – audio and video recordings on analogue or computer storage media, – computer games on computer storage media, – services provided by means of electronic communication, – educational services during which the course content is delivered by the instructor by means of electronic communication, – advertising services, in particular in newspapers, on posters and on television, – call centres, – educational services provided by correspondence, especially through the post, – conventional auction house services involving human intervention, irrespective of the bid submission mode, –

telephone services with a video component, – access to the internet, – telephone services provided via the internet (Journal of Laws of 2013, item 412).

In accordance with Article 2 (2) of Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services, a digital service means (a) a service that allows the consumer to create, process, store or access data in digital form, or (b) a service that allows the sharing of, or any other interaction with, data in digital form uploaded or created by the consumer or other users of that service, or other forms of interaction using such data. This definition incorporates both an element of the creative process of digital content and of its use. The extension of the definition of information society service providers will include internet service providers, cloud computing, domain name system service providers, social media, search engines, collaborative economy platforms, online advertising services, blockchain-based services. These are commonly referred to as ISPs (internet service providers), and these types of providers are already covered by sector-specific provisions, including the new European Electronic Communications Code (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, p. 36) and Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the BEREC Support Agency (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No. 1211/2009 (OJ L 321, p. 1), which is currently being implemented in EU countries. The global reach of digital services materially contributes to the fact that there is no full standardisation of legal relations relating to their provision. These are cross-border services, and domestic law cannot influence the services rendered by service providers from other countries. This also applies to the National Cybersecurity System Act although the Polish legislator has stipulated that the rules relating to cybersecurity obligations shall apply to a legal person or an organisational unit without legal personality having its registered office or management board in the Republic of Poland, or acting via a representative having its organisational unit in the Republic of Poland, provided that the digital service provider which does not have an organisational unit in one of the Member States of the European Union, but offers digital services in the Republic of Poland, shall appoint a representative having its organisational unit in the territory of the Republic of Poland, unless it has already appointed a representative having its organisational unit in another Member State of the European Union. A representative may be a natural person, a legal person or an organisational unit without legal personality, established in the Republic of Poland or in another European Union Member State, appointed to act on behalf of the digital service provider that does not have an organisational unit in the European Union, whom the authority competent for cybersecurity, the CSIRT MON, the CSIRT NASK or the CSIRT GOV may refer to in connection with the digital service provider's obligations under the Act. The definition of a digital service and the specification of its objectives will have an impact on determining the responsibility for the tasks which entail responsibility. This is how it was also envisaged in the draft Digital Services Act (Proposal – Regulation of the European Parliament and of the Council on a single market for digital services (Digital

Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.), under which digital services comprise a large category of online services, ranging from simple websites to online infrastructure services and online platforms. The principles set out in the draft of the Digital Services Act primarily concern online intermediaries and online platforms, such as online marketplaces, social networking sites, content sharing platforms, app stores, and online travel and accommodation platforms. In turn, the draft Digital Markets Act (Proposal – Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final) contains provisions governing online "gatekeeper" platforms. Gatekeeper platforms are digital platforms playing a systemic role in the internal market, which function as bottlenecks between businesses and consumers in the case of important digital services. Some of these services are also regulated under the Digital Services Act, but for different reasons and to different extents.

The types of digital services to which the reference regulation applies are set out in Annex 2 to the National Cybersecurity System Act. These are: **an online marketplace** – a service enabling consumers or traders to enter into contracts electronically with traders in an online marketplace or on the website of the trader who uses services provided by the online marketplace (e.g., Allegro, ING Usługi dla Biznesu S.A. – ALEO.COM, B2B automicob2b.pl platforms); **a cloud computing service** – a service enabling access to a scalable and flexible set of computing resources for a shared use by multiple users (such as Cloud for Business – ergonet.pl, Amazon Web Services, Google Cloud Platform, Microsoft Azure, private and hybrid clouds) and **a search engine** – a service enabling users to search all web pages or websites in a given language by entering a keyword, a phrase or another element as a query, and then presenting links that refer to information connected with the query. The users of digital services should encompass natural and legal persons who are customers of, or subscribers to, an online marketplace or a cloud computing service, or who are visitors to an online search engine website in order to undertake keyword searches (Commission Implementing Regulation (EU) 2018/151). The measures to be launched by digital service providers must ensure a level of cybersecurity appropriate to the risk, taking into account the following elements: 1) the security of systems and facilities; 2) incident handling; 3) business continuity management; 4) monitoring, auditing and testing; 5) state of the art, including compliance with international standards, as referred to in Commission Implementing Regulation (EU) 2018/151.

When analysing cybersecurity issues in the context of responsibility for the security of digital services, it is important to pay attention to the transmission of data and information by electronic means, the ICT network. One can say that cybersecurity law, including that dealing with the security of the information itself, touches upon issues related to the legal protection of the ICT system that contains certain data enabling the provision of digital services, the protection of the electronic services themselves and related content and databases, as well as the network through which the transmission of such services takes place. Therefore, it should be assumed that cybersecurity is closely related to the notions

of information and telecommunication security, and more specifically to ICT security, which means the protection of information processed, stored and transmitted using ICT systems against undesired (either accidental or intentional) disclosure, modification or destruction, or against rendering its processing impossible. Digital service providers may submit to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV information regarding: 1) other incidents; 2) cyber threats; 3) risk estimation; 4) vulnerabilities; and 5) technologies used. "Cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons (Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1 OJ L 151, 7.6.2019, pp. 15–69). This is not a mandatory obligation, but it is related to the possibility of ensuring the fulfilment of other tasks of the digital service provider, which, through the scope of the information provided, can contribute to improving the level of cybersecurity.

3 Digital infrastructure and the proposal for a CER Directive

Another area of future regulations covering the duties and responsibilities of online platforms is the area of crisis management. The Proposal for a Directive of the European Parliament and of the Council on the critical entities resilience (CER) of 16 December 2020 COM(2020) 829 final 2020/0365(COD). As is stressed by the EU legislator in the Proposal, "the current framework on critical infrastructure protection is not sufficient to address the current challenges to critical infrastructures and the entities that operate them. Given the increasing interconnection among infrastructures, networks and operators delivering essential services across the internal market, it is necessary to fundamentally switch the current approach from protecting specific assets towards reinforcing the resilience of the critical entities that operate them". The Proposal, therefore, introduces new duties to adopt certain measures to ensure the provision of services which are essential for the maintenance of vital societal functions or economic activities within the internal market, and in particular to identify critical entities and to enable them to comply with specific obligations in order to increase their resilience and improve their ability to provide these services within the internal market. The Directive also establishes rules on the supervision and the enforcement of critical entities and the specific oversight of critical entities considered to be of particular European significance. Article 1 further explains the relationship between the directive and other relevant acts of Union law, and the conditions under which information that is confidential pursuant to Union and national rules shall be exchanged with the Commission and other relevant authorities. These duties relate to the so-called digital infrastructure which includes, according to the subjective definition, providers of cloud computing service (referred to in point (X) of Article 4 of NIS 2 Directive); providers of data centre service (referred to in point (X) of Article 4 of NIS 2 Directive); and providers of content delivery network (referred to in point (X) of

Article 4 of NIS 2 Directive). A content delivery network is a network of servers that deliver websites and other content to users.

4 Responsibility of online platforms for digital content

The processes of the convergence of digital media with traditional media has given rise to a particular type of conflict regarding arrangements for the scope and level of new regulations, particularly with respect to digital content in the case of which most issues relate to new media and new technologies (the protection of intellectual property, protection of national identity, right to privacy, the protection of children and young people), as well as in the economic field (control of the media market and the responsibility of digital service providers). New content management models are seen to emerge (including online), supported by new principles of virtual organisation.

Technological change in the field of communication has fundamentally modified the ways individuals and entire communities function. Online multimedia platforms providing electronic services are being launched, which require the use of modern technological solutions, with investments being most frequently made by entities operating in the private sector. An open and free cyberspace allows the exchange of cultures and experiences between countries, communities and citizens, enabling interaction and the sharing of content and, in consequence, also knowledge, experiences and technologies. The ideological basis supporting this exchange is the freedom of speech and the freedom of communication. Digital reality facilitates the implementation of public tasks in a new social dimension (On the redefinition of public interest in the new media, see Chałubińska-Jentkiewicz, Nowikowska, Wąsowski, 2020). The new technological order constitutes the premise and, at the same time, the subject of the discussed changes, which fundamentally impact on the regulatory area of digital media. The issue of regulating this domain of activity refers to several main levels. The activity of digital content providers entails making that content available through ICT systems. This category is strongly diversified, covering not only specialised institutions or entities but also end users. The latter group is particularly active due to the growing popularity of user-generated sites (or user-generated content). Due to their intensive activities online, content providers bear direct liability for any infringements resulting from such activities.

In the current Polish legal system, content providers also bear direct liability for infringements upon third-party rights. As noted by J. Barta and R. Markiewicz, attempts to classify the activities consisting in making works available in computer networks gave rise to controversies, and these activities were eventually qualified as a new field of use, i.e., making a work available in such a way that everybody could access it at a time and place chosen by them. In ICT networks, the functioning of which is based on interactivity, this issue was of significant importance, while the modification of content and its further dissemination by users, in the course of digital processes, did not prove troublesome. The concept of *sui generis* protection of the rights of the producer or provider of content on the network appears interesting.

5 The liability of digital content intermediaries

As regards other infringements, content providers were considered parties directly committing the infringement and were thus excluded from the limitation of liability of providers of electronically supplied services. Not only did technological changes influence the scope of liability for illegal acts in cyberspace, but also new rules emerged to limit that liability. In European law, the liability of internet service providers is regulated by way of Directive 2000/31/EC, which contains provisions regarding the most popular network services: *mere conduit*, *caching* and *hosting*. Similar rules of liability were also upheld in the proposed Digital Services Act. It should be noted that the European regulation follows the horizontal model, meaning that the exemptions it provides for apply to any legal liability, including civil, criminal, and administrative liability. Directive 2000/31/EC on Electronic Commerce lays down the rules for excluding liability at the maximum level. Consequently, individual Member States may decide to impose less strict solutions. The provisions of Directive 2000/31/EC on Electronic Commerce were transferred into Polish law by way of Articles 12–15 of the APSEM. Under Article 12 of that Act, relating to mere conduit, "the service provider that provides services by electronic means involving transmission in a telecommunications network of data shared by the recipient of the service or the provision of access to a telecommunications network, within the meaning of the Act of the 16 July 2004 – Telecommunications Law, shall not bear responsibility for the conveyed data if: 1) it is not an initiator of the transmission; 2) does not select the recipient of data; and 3) does not delete or modify the data being subject to transmission". The releasing from responsibility, referred to in paragraph one, also covers automated and short-term indirect storage of the transmitted data, if this activity aims exclusively at proceeding with transmission, and the data are not stored longer than necessary for the accomplishment of the transmission in ordinary conditions (Article 12(2) of the APSEM).

6 Editorial responsibility for digital content

The basic regulatory provisions on the digital media market, and in particular large corporations (online platforms), were laid down in the First Amendment to the U.S. Constitution, where it was established that Congress should make no law restricting the freedom of speech or the freedom of the press, and in Article 230 of the Communications Decency Act (47 U.S. Code), which reads that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". This provision ultimately stipulated that the intermediary does not bear editorial responsibility for the content it shares when providing a digital service. Therefore, this rule is equally applicable to all activities related to a platforms operation in the context of the American law by which they are governed. However, it should be noted that, also in the context of libel, certain legal acts have been issued, such as Rachel's Law (in New York State, in connection with the case of Dr Rachel Ehrenfeld, an American researcher who was sued in London by a Saudi

businessman and his two sons over a book which, although not published in the UK, was sold in 23 copies via the internet and one chapter was made available online (cf. Garton Ash, 2018: 48–49). In Ehrenfeld v. Mahout, the Supreme Court of the New York State held that the law would not protect Dr Ehrenfeld from a British lawsuit filed by Saudi billionaire Khalid Salim Bin Mahfouz, where she was ordered to pay over $225,000 in damages and legal fees to Bin Mahfouz, as well as to apologise and destroy existing copies of her books), and the SPEECH Act (Libel Terrorism Protection Act, S.6687/A.9652), which protects American citizens from the impact of foreign libel judgements if these fail to satisfy the First Amendment or procedural standards. According to R. Lancman: "This law will give New York's journalists, authors, and press the protection and tools they need to continue to fearlessly expose the truth about terrorism and its enablers, and to maintain New York's place as the free speech capital of the world" (cf. Garton Ash 2018:48-49).

It should further be noted that on29 April 2021 the European Parliament and the Council of the EU adopted a regulation to prevent the online dissemination of terrorist content (Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ EU L 172, p. 79). The Regulation is to take effect in 2022. It stipulates that domestic bodies responsible for countering terrorism will not need to obtain prior judicial authorisation to order the removal of terrorist content, and a domestic body of a Member State will be able to demand the removal of content uploaded on a platform belonging to any provider rendering its services within the EU in all EU countries. An obligation was introduced for platforms to remove terrorist content within one hour (unless this is deemed impossible due to "technical issues").

An exception was made for educational, journalistic, scientific, artistic and other content whose purpose is not to promote terrorism but to spread awareness of the dangers of terrorism. The underlying issue is whether automated filters will be capable of distinguishing such content from genuinely harmful publications. The Regulation introduces a mechanism of appealing against unjust decisions to remove content (which is, in principle, intended to enable restoring such content and thus counteracting the phenomenon of excessive and arbitrary blocking) and an obligation for internet corporations to publish reports (allowing for the monitoring of how the Regulation will be applied in practice). As previously mentioned, the Digital Services Act introduces new general rules on the liability of, *inter alia*, platforms for content added by their users, this change being consistent when it comes to the liability of intermediaries on the digital services market. In accordance with the new regulations, platforms will have a maximum of one hour to remove or block access to content marked as terrorist content (including texts, photos, audio or video recordings that incite, abet or contribute to terrorist crime, contain instructions facilitating the commission of terrorist crime or incite participation in a terrorist group). This implies that although platforms will not be under the obligation to monitor or filter content on an ongoing basis, if the domestic bodies identify a site as being particularly exposed to terrorist propaganda, it will be obligatory to take measures

to prevent the publication of such content. The Regulation, however, does not specify in detail the measures to be taken, so it will be up to the platform whether it decides to use algorithms to filter content or hire moderators to do so.

The responsibility of a content-sharing internet-portal administrator for users' comments appears equally doubtful. More specifically, doubts arise as to the qualification of such comments as press material within the meaning of Article 7 (2)(1), and (4) & (5) of the Press Law. Press material means any text or image published or submitted to a publication, whether informative, journalistic, documentary, or other, regardless of the media means, type, form, destination, or authorship. At the same time, based on the applicable legislation, the press is construed as including periodical publications which do not constitute a limitative or homogeneous entirety, are published at least once a year, and bear a permanent title or a name, a number and a date, including in particular daily newspapers and magazines, news wires, telex messages, bulletins, radio and television broadcasts, or newsreels. It also covers any means of mass media, existing and emerging in the course of technological advancement, including broadcasting stations and PA systems, which distribute periodical publications via print, video, audio, or any other broadcasting means, as well as teams of people and individuals engaging in journalistic activity.

In this context, Strasbourg case law uses the term "public watchdog" when referring to the vital role played by the press. The principle that the freedom of expression, and the resulting free public debate, constitutes one of the essential foundations of a democratic society, and one of the basic conditions for its progress, and for every individual's self-fulfilment, forms one of the case-law principles adopted by the European Court of Human Rights. However, in case 5493/72, Handyside v. the United Kingdom (ECHR Judgement of 17 December 1976, 5493/72, Handyside v. the United Kingdom, HUDOC), the Court ruled that the freedom of expression was applicable not only to information or ideas which are favourably received or regarded as inoffensive, or as a matter of indifference, but also to those which offend, shock, or disturb the State, or any sector of the population. Such are the demands of the pluralism, tolerance, and broadmindedness, without which there is no democratic society. A similar view was highlighted by the Court of Justice of the European Union under Article 10 of the European Convention on Human Rights, and in Article 11(1) of the Charter of Fundamental Rights (cf. Judgements of the Court of Justice of 6 March 2021, C-274/99 P, Bernard Connolly v. the European Commission EU:C:2001:127; Judgement of 13 December 2001, C-340/00 P, the European Commission v. Michael Cwik, EU:C:2001:701; of 6 September 2011, C-163/10, criminal proceedings against Aldo Patriciello, EU:C:2011:543; Judgement of 3September 2014, C-201/13, Johan Deckmyn and Vrijheidsfonds VZW v. Helena Vandersteen et al., EU:C:2014:2132.). The same view should also be considered to form part of the case law of the Constitutional Tribunal of the Republic of Poland (cf. Judgements of the Constitutional Tribunal of 23 March 2006, K 4/06, OTK-A 2006/3, item 32; of 11 October 2006, P 3/06, OTK-A 2006/9, item 121; of 30 October 2006, P 10/06, OTK-A 2006/9,

item 128; of 14 December 2011, SK 42/09, OTK-A 2011/10, item 118; of 25 February 2014, SK 65/12, OTK-A 2014/2, item 14).

This view is shared in the rulings of the Supreme Court. It is indicated that a journalist's obligation to exercise diligence and accuracy arising from Article 12(1) of the Press Law Act (the Press Law Act refers to due diligence and accuracy) means qualified diligence and accuracy which takes into consideration the actual role of the media in a democratic society, and in their tangible impact on public opinion, and hence the emerging threats to the information autonomy and moral rights of individual people (see Resolution of the Supreme Court (7) of 18 February 2005, III CZP 53/04, LEX No. 143120). Also in the rulings of the Constitutional Tribunal, the emphasis is on the significant correlation and interrelation of the media's freedom of expression, and their responsibility for exercising that freedom, as well as the resulting need to ensure the appropriate protection of other constitutional values, including the moral rights of third parties (see in particular the judgements of the Constitutional Tribunal of 12 May 2005, SK 43/05, OTK-A 2008/4, item 57, and of 30 October 2006, P 10/06, OTK-A 2006/9, item 128).

Considering the above, in the judgement passed in case 64569/09, Delfi v. Estonia (ECHR Judgement of 16 June 2015, 64569/09, Delfi AS v. Estonia, LEX No. 1730680), the European Court of Human Rights ruled that making the internet news portal responsible for offensive comments posted on its site was legitimate. The court thus claimed that, notwithstanding the provisions of Directive 2000/31/EC on Electronic Commerce, specific solutions might be adopted in domestic law limiting the freedom of expression if the internet users' comments are offensive or hateful, and the portal administrator has failed to prevent their publishing, has derived benefits from such publishing, and has ensured the anonymity of their authors. Under that interpretation, the exclusions made in Articles 12–15 of the APSEM are subject to analysis, including in the context of other regulations governing the protection of human rights and freedoms.

Due to the fact that comments posted by anonymous authors on an online portal administrated by a website can include content violating moral rights, the responsibility in the context of violating the provisions of Article 24 § 1 of the Civil Code should be subject to scrutiny. The Supreme Court, in its judgement of 30September 2016, I CSK 598/15 (LEX No. 2151458), adopted the view that the provisions of Article 14(1) and (15) of the APSEM govern issues related to the exclusion of the online portal administrator's liability, but they fail to regulate such issues as apportioning the burden of proof, and the absence of illegality of actions of the online portal administrator rendering hosting services. The Supreme Court highlighted that, under Article 24 § 1 of the Civil Code, any person whose personal interests are threatened by another person's actions may demand that these actions be ceased. If there is an infringement, he or she may also demand that the person committing the infringement take the necessary steps to remove its effects, in particular that the person makes a statement of the appropriate form and substance. Moreover, Article 24 § 1 of the Civil Code does not restrict its applicability to parties directly committing the infringement of moral rights, who in this case are

anonymous authors, but also covers all the activities of entities which in any way infringe or contribute to infringing the moral rights of the aggrieved party, or aggravate the infringement of such rights caused previously by other entities (under this provision, the notion of the party committing the infringement of moral rights is broad enough to make referring to Article 422 of the Civil Code unnecessary). The Supreme Court noted that the freedom of expression exercised on internet fora by anonymous authors often provokes uncontrollable expressions which evolve into hate speech infringing on the moral rights of third parties. Finally, the Supreme Court stressed that individuals who are offended and slandered in anonymous posts, when the liability of the parties who directly commit the infringement is excluded, find themselves at a particularly greater legal disadvantage. "Such an aggrieved party does not even have to have access to the internet, or "read" websites, or spend their time looking for posts which are offensive or slanderous to them, or which undermine their authority. It is possible that an individual who does not use the internet might even never learn about the illegal anonymous posts about him or her which irreversibly undermine their integrity. The internet is a medium which should be friendly to the information society by design. Therefore, effective legal mechanisms should be in place to prevent the use of the internet for insulting the dignity and honour of citizens without any legal consequences for the perpetrators". Accordingly, the defending party bears the burden of proof that before the lawsuit was served, it had had no knowledge of the incriminating comments posted by internet users.

It needs to be stressed that the exclusion of civil-law liability is governed both by Article 24 § 1 of the Civil Code, and the aforementioned Article 14(1) and Article 15 of the APSEM. Assessing the interrelation of these provisions, therefore, appeared justified. However, the Supreme Court decided not to make that assessment, which influenced its judgement. This extended interpretation might seem contradictory to the conflict-of-law rules, the principle of legal-system consistency, and the interpretation of the objectives of the provisions, both as regards Directive 2000/31/EC on Electronic Commerce and the Act on the Provision of Services by Electronic Means. In this context, the provision of Article 14(1) of the APSEM might appear groundless. However, the justification of the above-mentioned ruling is congruent with the recent Commission Recommendation (EU) which deals with the monitoring of content made available as part of a hosting service. Pursuant to Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online, provisions should be made for mechanisms to submit notices. These mechanisms should be easy to access, user-friendly and should allow the submission of notices by electronic means. More specifically, these mechanisms should allow the submission of notices which are sufficiently precise and adequately substantiated to enable the hosting provider concerned to take an informed and diligent decision in respect of the content to which a given notice relates, in particular whether or not that content is to be considered illegal, and whether or not it is to be removed or access thereto is to be disabled. These mechanisms should be such as to facilitate the provision of notices that contain an explanation of the reasons why the notice provider considers that content to be illegal and a clear indication of the location of that content. Where the notice providers decide to do so, their anonymity should be ensured towards the content

provider. Where a hosting service provider decides to remove or disable access to any content that it stores because it considers the content to be illegal, irrespective of the means used for detecting, identifying or removing or disabling of access to that content, and where the contact details of the content provider are known to the hosting service provider, the content provider should, without undue delay, be informed in a proportionate manner of that decision and of reasons for taking it, as well as of the possibility to contest such a decision. Content providers should be given the possibility to dispute the decision by the hosting service provider, at a reasonable time, through the submission of a counter-notice to that hosting service provider. The mechanism to submit such counter-notices should be user-friendly, and allow their submission by electronic means.

It should be ensured that hosting service providers process the received counter-notices in the proper manner. When the counter-notice contains grounds for the hosting service provider to consider that the content to which the counter-notice relates is not to be considered illegal, it should reverse its decision to remove or disable access to that content without undue delay, without prejudice to its possibility to set and enforce its terms of service in accordance with Union law and the laws of the Member States. Hosting service providers should be encouraged to take, wherever appropriate, proportional and specific proactive measures in relation to illegal content. Such proactive measures could involve the use of automated means for the detection of illegal content only where appropriate and proportionate, subject to effective and appropriate safeguards. The removal of content which is not illegal should be precluded, without prejudice to the possibility for hosting service providers to set and enforce their terms of service in accordance with Union law and the laws of the Member States. To this end, there should be effective and appropriate safeguards ensuring that hosting service providers act in a diligent and proportionate manner in respect of content that they store, in particular when processing notices and counter-notices and when deciding on the possible removal of or the disabling of access to content considered to be illegal content.

Where hosting service providers use automated means in respect of the content they store, effective and appropriate safeguards should be provided to ensure that decisions taken concerning that content, in particular decisions to remove or disable access to content considered to be illegal, are accurate and well-founded. The document also contains detailed recommendations concerning terrorist content. Hosting service providers should expressly set out in their terms of service that they will not store illegal content and should take measures so that they do not store terrorist content.

7 The proposed Digital Services Act – new rules of liability of digital content intermediaries

The proposed Digital Services Act retained the rules of liability of network service providers and intermediaries, laid down in Directive 2000/31/EC on Electronic Commerce which is considered the basis for the digital economy. Nevertheless, to ensure

an effective harmonisation across the European Union and to avoid legal fragmentation, it was considered necessary to include these rules in the regulation. It was also deemed appropriate to clarify some aspects of these rules to eliminate the existing disincentives towards voluntary own-investigations undertaken by providers of intermediary services in order to ensure their users' safety, and to clarify their role from the perspective of consumers in certain circumstances. Chapter II of the proposed Act contains provisions on the exemption from liability of providers of intermediary services. More specifically, it stipulates the conditions under which providers of mere conduit (Article 3), caching (Article 4), and hosting services (Article 5) are exempt from liability for the third-party information they transmit and store.

The proposed DSA introduces the following regulations:

- measures against illegal goods, services, or content on the internet, such as a mechanism enabling users to flag such content, and, as regards platforms, a mechanism for cooperation with "trusted flaggers",
- new duties related to the traceability of business users of online marketplaces in order to make it easier to trace the sellers of illegal goods,
- effective safeguards for users, including the possibility to contest a platform's decisions regarding content moderation,
- extensive measures to ensure the transparency of online platform operations, including algorithms used for prompts,
- duties imposed on very large platforms to prevent the improper use of their systems by taking measures based on risk assessment, and by conducting independent inspections in connection with systems risk management,
- ensuring that the largest platforms provide scientists with the most important data in order to facilitate research into how threats evolve on the net,
- a supervisory structure matching the complexity of online space: EU countries will play a major role, supported by the new European Council for Digital Services, and in the case of very large platforms – enhanced supervision and provisions enforcement by the Commission.

It was noted in the Regulation that the platforms are deemed obligated if their reach exceeds 10% of the European population, i.e., 450 million consumers.

The proposed Act also introduces the previously known rules of limited liability for content in cases of mere conduit, caching, and hosting.

The proposed Act also introduces a rule stating that exemptions from liability of the providers of intermediary services should not be waived if they carry out voluntary or legally required own-initiative investigations (Article 6). The proposed Act further provides that no general obligation to monitor the information should be imposed on these providers (Article 7). In addition, the proposed Act imposes an obligation on the providers of intermediary services to enforce, as appropriate, orders issued by the relevant national

judicial or administrative authorities regarding illegal content (Article 8), and to furnish information (Article 9).

The proposed Act also contains a definition of illegal content, which stands for any information that, in itself or by its reference to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law (i.e., referring to content considered illegal under the provisions of media law, hate speech or copyright). A definition of dissemination to the public is also introduced, referring to making content available, at the request of the recipient of the service who provided the content, to a potentially unlimited number of third parties. The proposed Act defines the term "online platform" as a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another, and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this regulation. The term "content moderation" is considered to mean the activities undertaken by providers of intermediary services aimed at detecting, identifying, and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken which affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of the recipient's account.

In compliance with the Polish standpoint on adopting the proposed Digital Services Act, the rule of the limited liability of online intermediaries (liability exceptions) should be upheld. The conditions to release the intermediary from liability should still include having no knowledge of the illegal character of the content, and removing or effectively preventing access to such content by the intermediary once it becomes aware of its illegal character. At the same time, the Digital Services Act should envisage penalties for those digital service providers which do not react appropriately to notices regarding illegal content. The requirement of the intermediary's neutrality towards illegal content as a prerequisite to being exempt from responsibility for users' content should be dropped, as it no longer matches the reality. Attention was rightfully drawn in that standpoint to the fact that, under the current digital-market conditions, the degree of activity in respect of content forms part of the service provision – for instance, in the context of the processing of personal information generated passively. The new solutions should combine a platforms' actions in identifying and removing illegal content with the protection against making them automatically responsible for the content disseminated via their services by third parties, including users. One of the solutions is to introduce the so-called "Good Samaritan" clause.

The introduction of the "Good Samaritan" rule referred to in recital 25 and Article 6 , under which the intermediary should not be punished for merely carrying out activities,

in good faith, aimed at removing illegal content, going beyond the obligations arising from the applicable Acts or regulations. What is more, intermediaries should be encouraged to do so. Nonetheless, it is worth making it even clearer that this rule does not exempt the intermediary from responsibilities arising from the obligation to react appropriately under the notice and action procedure, and as a result of receiving an order from the authorised body. The provisions must make it clear that the application of the "Good Samaritan" rule by a given intermediary is not automatically equivalent to its being exempt from any liability in any situation. The use of the proactive "Good Samaritan" measures by an intermediary should not, in principle, prevent it from using the exemption from liability, but it must not lead to a situation in which the intermediary invokes the "Good Samaritan" rule to evade liability, despite the fact that it takes other measures that would normally qualify under the liability principles of the proposed regulation. In line with recital 25: "In order to create legal certainty and not to discourage activities aimed at detecting, identifying and acting against illegal content that providers of intermediary services may undertake on a voluntary basis, it should be clarified that the mere fact that providers undertake such activities does not lead to the unavailability of the exemptions from liability set out in this Regulation, provided those activities are carried out in good faith and in a diligent manner. In addition, it is appropriate to clarify that the mere fact that those providers take measures, in good faith, to comply with the requirements of Union law, including those set out in this Regulation as regards the implementation of their terms and conditions, should not lead to the unavailability of those exemptions from liability. Therefore, any such activities and measures that a given provider may have taken should not be taken into account when determining whether the provider can rely on an exemption from liability, in particular as regards whether the provider provides its service neutrally and can therefore fall within the scope of the relevant provision, without this rule however implying that the provider can necessarily rely thereon."

The Digital Services Act proponent has also decided not to impose a general obligation on online intermediaries to monitor information posted by users. However, it is worth noting that the proponent has not waived the monitoring obligation in specific cases, though it has done so only in recital 26 and not in the main provisions of the regulation. According to that recital: Where possible, third parties affected by illegal content transmitted or stored online should attempt to resolve conflicts relating to such content without involving the providers of intermediary services in question. Recipients of the service should be held liable, where the applicable rules of Union and national law determining such liability so provide, for the illegal content that they provide and may disseminate through intermediary services. Where appropriate, other actors, such as group moderators in closed online environments, in particular in the case of large groups, should also help to avoid the spread of illegal content online, in accordance with the applicable law. Furthermore, where it is necessary to involve information society services providers, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the actor that has the technical and operational ability to act against specific items of illegal content, so as to prevent and

minimise any possible negative effects for the availability and accessibility of information that is not illegal content".

It is worth noting that, in line with recital 27, "services used for communications purposes, and the technical means of their delivery, have also evolved considerably, giving rise to online services such as Voice over IP, messaging services and web-based e-mail services, where the communication is delivered via an internet access service. Those services, too, can benefit from the exemptions from liability, to the extent that they qualify as mere conduit, caching or hosting service".

Other significant obligations arise from Articles 13 and 23 of the proposed Act, referring to transparency and reporting which should not violate business secrets, the confidentiality of commercial contracts, or user privacy. Transparency does not need to involve publicly disseminating detailed data and all the information required to the extent that they involve trade secrets or confidentiality. Such information and data should be provided only via reports addressed to supervisory bodies and the European Commission. The European Commission should ensure that the reporting rules are just, proportionate, and uniform, in all EU countries.

Under Regulation EU No. 524/2013 on online dispute resolution for consumer disputes, the right to use the online dispute resolution (ODR) platform was introduced. This is a European platform to be used by ADR (alternative dispute resolution) entities. Consumers must be notified of such a dispute resolution procedure, and the online store website must contain a link to the online platform.

In the process of the notifying of illegal content, it is important that the status of *trusted flagger* is awarded by the Digital Services Coordinator, which will not only enable the reliable verification of the entities applying for such a status, but will also facilitate eliminating entities intending to take measures in bad faith, while aligning the requirements with domestic needs, taking into consideration the public interest also dictated by public morality characteristic of a given community. It would seem advisable to enhance trusted flaggers in the context of the removing/blocking of the notified content by the platform. Notices submitted by trusted flaggers should be processed and decided on with priority in relation to notices submitted by ordinary users (as stipulated in Article 19 (1)), and they should be justified and monitored. In fact, Article 20 of the proposed Act authorises online platforms to take action against users and entities posting illegal content, or frequently submitting unjustified notices. These increase the legal certainty of platform operations, considering that a specific platform operation in such cases will not be based exclusively on the platform's terms and conditions which the users may challenge, but on explicit legal regulations.

The obligation for e-commerce platforms to identify the trustworthiness of business users (traders) will contribute to increasing users' confidence in online shopping, and to reducing the posting of illegal products, services, and content on these platforms, which

can make an important contribution to the identification efforts in the context of increased cybercrime. Data retention not envisaged in the Directive is important in the efforts to combat cybercrime. The retention of such data for two years for investigative purposes would enable the much more effective detection of crimes related to the provision of illegal products, content, and service.

8 Notifications and other mechanisms of intermediaries' activities

Intermediary services offering network infrastructure include internet access providers, domain name registries, hosting services such as cloud-based services and webhosting. Online platforms, such as online marketplaces, app stores, social networking and sharing platforms, and very large online platforms pose a particular risk when it comes to disseminating illegal and socially harmful content. The providers of hosting services are obliged to put mechanisms in place to allow any individual or entity to notify them of the presence on their service of illegal content. These mechanisms should be easy to access, user-friendly, and facilitate the submission of notices exclusively by electronic means. To that end, the providers should take the necessary measures to enable the submission of notices containing all of the following elements:

- an explanation of the reasons why the content is considered illegal;
- a clear indication of the electronic location of that information, in particular the exact URL or URLs, and, when necessary, additional information enabling the identification of the illegal content;
- the name and an electronic mail address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/UE;
- a statement confirming the good-faith belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete.

The Digital Services Act significantly enhances the mechanisms for illegal-content removal, and the efficient protection of fundamental internet users' rights, including the freedom of expression. It also increases the level of public control over the activities of online platforms, especially including those used by more than 10% of the EU population. Online platforms provide recipients of the service, for a period of at least six months, with access to an effective internal complaints handling system, which enables the complaints to be lodged electronically and free of charge, against decisions taken by the online platform on the basis that the information provided by the recipients is illegal content, or incompatible with its terms and conditions. This relates to online platforms which provide services to a large number of monthly active recipients (45 million or more), which is verified at least every six months by the Digital Services Coordinator.

It is worth adding that the service provider's liability is closely related to the status of knowledge of the unlawfulness of a given action (Gołaczyński, 2009 , Rączka, 2009). In the judgement of 18January 2011, I ACa 544/10 (LEX No. 736495), the Appellate Court

in Lublin adopted a standpoint that while the service provider is under no obligation to monitor its network, nor is it obliged to take measures to implement monitoring software, once it becomes aware of any infringement, or its illegal character, liability is to be undoubtedly considered to have arisen on the part of that provider.

The inclusion of the service provider's liability is not conditional on the exercising of diligence involving in particular the control of stored data. Article 15 of the APSEM stipulates that the entity which provides services specified in Articles 12–14 is not obliged to monitor the data referred to in these articles, which are transmitted, stored, or made available by that entity. Theoretically, this is because the suppliers of electronic services only provide an ICT base, and have no control over what is made available within the service. Thus, the issue of a service provider's lack of liability applies when they have no knowledge of the illegal content stored with them. However, in a different situation, when service providers become aware of such data (either on the basis of reliable information or as a result of official notification) – they are obliged to promptly block access to it. Service providers are then obliged to control the content of the stored data, which seems to be in conflict with the provision of Article 15 of the APSEM. Therefore, it may be argued that providers of electronic services, which include transmission, via the telecommunication network, of data supplied by the service recipient, or the provision of access to the telecommunication network, may be released from any liability towards third parties, and, in addition, that they are not under any statutory obligation to monitor the content of the service on an ongoing basis, in order to detect any illegal content (pursuant to Article 15 of the APSEM). However, as already indicated, this does not exclude the liability of instigators, helpers, or persons who knowingly take advantage of damage caused to others(Article 422 of the Civil Code).

9 The liability of video-sharing platform operators

Amendments to the Audiovisual Media Services Directive 2010/13/EU, by way of Directive 2018/1808, introduce certain obligations, including for a video-sharing platform operator with a registered office in the territory of a Member State, within the meaning of Article 3(1) of Directive 2000/31/EC. In compliance with Article 28a(3) of Directive 2010/13/EU, it is considered that a video-sharing platform operator has its registered office in the territory of a Member State for the purposes of Directive 2000/31/EC if a) it has a parent or subsidiary with a registered office in the territory of a Member State, or b) it is part of a group, and another unit of that group has its registered office in the territory of the Member State.

Member States prepare and keep updated a list of video-sharing platform operators with registered offices in their territories, or regarded as having a registered office in their territory, and identify the criteria on which their authority is based. Member States submit the list and its updated versions to the Commission. The Commission ensures that such lists are shared on a central database. In the case of any inconsistency between the lists, the Commission contacts Member States in order to seek a solution. The Commission

provides access to the database to national authorities or regulatory bodies (Article 28a(6) of Directive 2010/13/EU).

The appropriateness of measures is determined by considering the nature of the content, the damage it can do, and the attributes of the categories of people subject to protection, as well as endangered rights and legitimate interests, including the rights and interests of video-sharing platform operators and the users who create or publish content on such platforms, as well as the general public interest. The measures must be workable and proportional, taking into account the size of the video-sharing platform and the nature of the service provided. These measures lead neither to *ex ante* control nor to the filtering of content on posting it onto a platform if it runs contrary to Article 15 of Directive 2000/31/EC. For the purposes of the protection of minors, as referred to in Article 28b(1)(a) of Directive 2010/13/EU, the most harmful content is subject to the harshest access control measures. Member States may take measures aimed at blocking websites which either include or disseminate child pornography among internet users on their territories. These measures must be introduced based on a transparent procedure, and provide sufficient guarantees, especially in order to ensure that the blocking is limited to what is necessary and appropriate, and to inform users about the reason for blocking. The guarantees might also include the possibility to obtain court compensation.

The governmental draft Act on amending the Broadcasting Act and the Act on Cinematography (9th term of office, Sejm paper No. 1340) stipulated that, in compliance with Directive 2018/1808, video-sharing platform operators do not bear editorial responsibility. It should be assumed that the issue of exclusion of editorial responsibility applies only to the audiovisual content made available by the user, and not to any content available on the platform or the way it is organised.

In line with the definition provided in the Polish Broadcasting Act, "a video sharing platform is a service provided by electronic means, as part of business activity conducted in this area, the primary purpose of which (or of its severable part) is to provide the general public with programmes or user-generated videos, for informational, entertainment or educational purposes, for which the service provider has no editorial responsibility but it decides on the method of compilation, including automatically or by means of algorithms, in particular by displaying, tagging, and sequencing". This appears to be a regulation that, while limiting editorial responsibility, does not collide with other rules imposing the liability of online intermediaries contained in the Directive on copyright and related rights in the Digital Single Market and the draft Digital Services Act.

It is forbidden to place broadcasts, user-created videos or other transmissions on video sharing platforms (under the Broadcasting Act, "other transmission" means all kinds of transmissions that are not broadcasts or user-created videos; this notion, therefore, includes commercial communications as well as other types of undefined communications, such as non-commercial information from non-governmental organisations, the so called board broadcasts (still images displayed on a screen) or

a sequence of sounds without an accompanying image in a TV programme), which: 1) prejudice the physical, mental or moral development of minors, in particular those containing pornographic or gratuitously violent content, without effective technical protection; 2) containing incitement to violence or hatred towards a group of people due to gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, nationality, membership of a national minority, property, birth, disability, age or sexual orientation; 3) containing content that may facilitate the commission of a terrorist crime, pornographic content with the participation of minors, content inciting to insult a group of people or an individual due to his/her national, ethnic, racial, religious affiliation or lack of religious denomination.

With the aim of implementing the above obligations, the video-sharing platform provider: 1) sets up and implements effective technical safeguards, including parental control systems or other appropriate measures, in order to protect minors from access to broadcasts, user-generated videos or other transmissions that prejudice the physical, mental or moral development of minors, in particular those containing pornographic or gratuitously violent content; 2) enables users of a video sharing platform to qualify the broadcasts, user-generated videos or other transmissions posted by them, and to apply technical safeguards to the broadcasts, user-generated videos or other transmissions posted by them. The National Council, by way of a regulation, may set up detailed requirements to be met by effective technical safeguards or other appropriate measures, with a view to protecting minors from watching broadcasts, user-created videos or other transmissions, guided by the need to ensure the effective protection of minors from content harmful to them, taking into account technical possibilities, the degree of harmfulness of such broadcasts, user-created videos or other transmissions to minors in particular age categories and the specific nature of video-sharing platforms.

It is worth adding that on 20 June 2019 the European Parliament and the Council of the European Union adopted Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services. This regulation has been in force since 12 July 2020, introducing a number of legal regulations, crucial for the way internet services are provided. Their adoption was motivated by the desire to effect the inclusion of internet services into the same legal regime that applies to "traditional" audiovisual and telecommunications services. It defines the principles of the operation of online platforms and search engines. The need to adopt that regulation arose from the fact that the use of online intermediation services can be crucial for the commercial success of undertakings which use such services to reach consumers. In addition, online search engines can be important sources of internet traffic for undertakings which offer goods or services to consumers through websites. It was considered necessary to establish a set of mandatory rules at the Union level to ensure "a fair, predictable, sustainable and trusted online business environment within the internal market" (Wozniak, 2019:1-10).

An online search engine was defined as a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular

language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found, and the provider of an online search engine means any natural or legal person which provides, or which offers to provide, online search engines to consumers.

It should be stressed that Regulation 2019/1150 is applicable to business-to-business (B2B) relations: platforms which provide intermediary services and traders who sell goods or provide services thanks to that (*platform-to-business*, P2B, relations) (Article 2 of Directive 2019/1150). In contrast, Regulation 2019/1150 does not apply to business-to-consumer relations or to online payment services, nor to online advertising tools or online advertising exchanges (Article 1(3) of Regulation 2019/1150). It should be stressed that the online intermediation service must be an Information Society service, within the meaning of Article 1(1)(b) of Directive 2015/1535, that is to say, a service provided: 1) for remuneration, 2) at a distance, 3) by electronic means, and 4) at the individual request of a recipient of services. It is stressed in legal commentaries that services performed under *gig economy* will not exhibit such a character. The intermediation service was excluded from the definition of an Information Society service. This refers to situations where the intermediary service is merely ancillary to the main service, but without the online intermediary service the main service cannot be implemented. This is true, for instance, of Uber, BlaBlaCar or Airbnb, where the service provided is a composite service consisting of an electronically provided service, e.g., a service for matching passengers with drivers, and a non-electronically provided service, such as a transport service, where the primary service is transport and it is the transport that gives the service its economic meaning (Konarski, 2020:147-148). The obligations stipulated in Regulation 2019/1150 are binding on providers of online intermediation services. Under Article 2(3) of Regulation 2019/1150, a provider of online intermediation services means any natural or legal person which provides, or which offers to provide, online intermediation services to business users. These entities can be considered to include online auction sites (e.g., Allegro), online booking systems (e.g., Booking.com) social networking sites (e.g., Facebook), to the extent that they are used for business purposes, or search engines (Google) (Konarski, 2020:148). Among the most important obligations, which are primarily information obligations, imposed on providers of online intermediation services, the EU legislator has enumerated the following: 1) the obligation to ensure appropriate terms and conditions of use, and the procedure for amending them (Articles 3 and 8 of Regulation 2019/1150); 2) the obligation to set out the terms and conditions determining ranking (Article 5 of Regulation 2019/1150); 3) the obligation to provide a description of the technical and contractual access of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services (Article 9 of Regulation 2019/1150). Each Member State is to ensure the proper and effective enforcement of the Regulation. Member States shall lay down the provisions specifying the measures to be applied in the case of violations of Regulation 2019/1150

and shall ensure their enforcement. The measures envisaged must be effective, proportional and dissuasive.

10 Liability under Directive 2019/790 on Copyright on the Digital Single Market

Another example of regulation concerning the liability for content shared on the web is Directive 2001/29/EC, which introduces limitations on the liability for copyright breach. Article 5(5) of Directive 2001/29/EC creates the possibility to lay down exceptions connected with illegal use, and provided for in Article 5 (1)-(4) of Directive 2001/29/EC, including the exception for copies for private use as referred to in Article 5 (2)(b) of the Directive, dependent on fulfilling three conditions: 1) the exception is applied only in certain special cases, 2) does not breach the normal use of an original work of authorship, and 3) does not do unjustified damage to the reasonable interests of copyright subjects. The three conditions correspond, as follows from Recital No. 44 of Directive 2001/29/EC, to the international obligations of the Member States and the European Union, and more precisely, to the conditions relating to any limitations on copyright set out in Article 9(2) of the Berne Convention, commonly known as the "three-step test", repeated in Article 13 of TRIPS and in Article 10 of the WCT. This test shall also apply to the use of works on the web.

Notwithstanding the foregoing, the provision laid down in Article 17(4) of Directive 2019/790 on Copyright in the Digital Single Market remains a key measure, according to which, if not granted permission, online content-sharing service providers are liable for acts of public distribution not covered by permission, including making original works of authorship and other copyrighted items known to the public, unless they prove that: a) they have made every effort to obtain authorisation , and b) have made every effort – assuring the highest degree of professional care and conduct specific to the sector – to ensure the lack of access to respective original works of authorship and other copyrighted items, with reference to which rightholders have provided service providers with relevant and necessary information; and in every case c) acted without delay on receiving duly justified reservations from rightholders in order to block access to original works of authorship or other copyrighted items to which a reservation pertains, or to remove them from their websites, and made every effort to prevent their publication in the future in accordance with subparagraph b.

By evaluating whether a service provider fulfils the obligations referred to in Article 17(4) of Directive 2019/790, and in view of the principle of proportionality, one has to consider, among other things, a) the type, the audience, and scale of the services provided, and the kind of original works of authorship or other copyrighted items posted by the users of a service, and b) the accessibility of the appropriate and effective measures and their costs for service providers (Article 17(5) of Directive 2019/790). When the online content-sharing service providers are liable for public sharing, or for making content publicly known, on the terms set out in Directive 2019/790, Article 14(1) of Directive 2000/31/EC

should not apply to liability following from the provisions of this Directive concerning the use of protected content by online content-sharing service providers. That should not affect the application of Article 14(1) of Directive 2000/31/EC with reference to such service providers for purposes falling outside the scope of Directive 2019/790 (Recital 65 of Directive 2019/790). The same is true of the regulations regarding liability in the proposed Digital Services Act.

That regulation also introduces new rules for excluding liability of the service provider. This applies to information society services and excludes from the Directive such services as WhatsApp, even if they serve the same functions, for instance, as Facebook does. "[…] as well as providers of business-to-business cloud services and cloud services, which allow users to upload content for their own use, such as cyberlockers, or online marketplaces the main activity of which is online retail, and not giving access to copyright-protected content" (recital 62, clause 5, of Directive 2019/790). Such regulation excludes from the applicability of the Directive services such as Google Drive, Microsoft Drive and iCloud, despite the fact that they enable mutual content sharing. G. Spindler points out, however, that as a rule then the premise of access to a "large number" of works is not met (cf. Spindler, 2019:347, cited: Markiewicz, 2021:207) for infringement of exclusive rights to a work. An obligation was introduced to obtain authorisation from the rightholders of works and, where this is not obtained despite having made "all reasonable efforts, in accordance with high standards of professional diligence in the sector", to exclude liability, service providers are obliged to: a) prevent access to individual works and other protected subject-matter regarding which the rightholders submitted the relevant and necessary information to the service providers, and b) in each case duly notify the rightholders to block access to the exclusive subject-matter and to make every effort to prevent future posting.

Table 1: Liability of intermediaries

Legal act	Directive 2019/790	Directive 2018/1808	Digital Services Act
The obliged entity	The online content-sharing service provider means a provider of an information society service of which the main, or one of the main purposes, is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes.	The provider of a video-sharing platform service which means a service within the meaning of Articles 56 and 57 of the TFEU, when the primary purpose of that service (or of its severable part) is to provide the general public with broadcasts or user-generated videos, or both of these, for informational, entertainment or educational purposes – via the electronic communications network	The provider of an intermediary service which means one of the following services: a "mere conduit" service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;

		within the meaning of Article 2(a) of Directive 2002/21/EC – for which the video-sharing platform service provider has no editorial responsibility but it decides on the method of compilation, including automatically or by means of algorithms, in particular by displaying, tagging, and sequencing.	a "caching" service that consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request; a "hosting" service that consists of the storage of information provided by, and at the request of, a recipient of the service. An online platform means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation.
Scope of liability	If not granted permission, online content-sharing service providers are liable for acts of public distribution not covered by permission, including making original works of authorship and other copyrighted items known to	Video-sharing platform service providers are obliged to use appropriate measures in order to protect: a) minors against broadcasts, user-created videos, and audiovisual commercial	Mere conduit, caching, hosting Hosting service providers shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of

	the public, unless they prove that: a) they have made every effort to obtain permission, b) have made every effort – assuring the highest degree of professional care and conduct specific to the sector – to ensure the lack of access to respective original works of authorship and other copyrighted items, with reference to which rightholders have provided service providers with relevant and necessary information; and in every case c) acted without delay on receiving duly justified reservations from rightholders in order to block access to original works of authorship or other copyrighted items to which a reservation pertains, or to remove them from their websites, and made every effort to prevent their publication in the future in accordance with subparagraph b.	communications which could be harmful to their physical, mental, or moral development – in accordance with Article 6a(1) of Directive 2018/1808; b) the general audience against broadcasts, user-created videos, and audiovisual commercial communications which incite violence or hatred towards a group of people or a member of a group, for the reasons referred to in Article 21 of the CFR; c) the general audience against broadcasts, user-created videos, and audiovisual commercial communications which include content whose distribution is an act, qualifies as a crime under EU law, i.e., public incitement to commit a terrorist crime, as defined in Article 5 of Directive 2017/541, a crime connected with child pornography, as defined in Article 5(4) of Directive 2011/92/EU, and a crime motivated by racism and/or xenophobia, as defined in Article 1 of Framework Decision 2008/913/JHA. Member States may subject video-sharing platform providers to more detailed or stricter measures than those referred to in Article 28b(3) of Directive 2010/13/EU. In adopting such measures, Member States shall comply with the requirements set out in applicable Union law, such	information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means.

		as those set out in Articles 12–15 of Directive 2000/31/EC or Article 25 of Directive 2011/93/EU	
Filtering	Yes, but this results from the scope of liability and not directly from the provision.	Member States should ensure that all video-sharing platform operators should apply these kinds of measures in their jurisdictions. The measures must be workable and proportional, taking into account the size of the video-sharing platform and the nature of the service provided. These measures shall lead neither to *ex-ante* control nor to the filtering of content on posting it onto a platform if it runs contrary to Article 15 of Directive 2000/31/EC. For the purposes of the protection of minors, as referred to in Article 28b (1)(a) of Directive 2010/13/EU, the most harmful content is subject to the harshest access control measures such as: establishing and operating multiple user verification systems for video-sharing platforms to detect content which could be harmful to the physical, mental, or moral development of minors; establishing and operating easy-to-use systems enabling video-sharing platform users to assess the content referred to in Article 28b(1) of Directive 2010/13/EU; – ensuring parental control systems subject to end-user control to detect content which could be harmful to	Content moderation means the activities undertaken by providers of intermediary services aimed at detecting, identifying, and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken which affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of the recipient's account. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear and unambiguous

		the physical, mental, or moral development of minors.	language and shall be publicly available in an easily accessible format. Such information shall be formulated in a clear and unambiguous manner and shall be provided to the public in an easily accessible format.
Blocking	The provider is obliged to block access to a given file or remove it from its websites by way of: 1) monitoring the content available on a given platform, and 2) the file containing an illegally located work being detected by the rightholders, and 3) monitoring the platform content after removing the file concerned.	None	Providers of intermediary services shall, upon the receipt of an order to act against a specific item of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union or national law, in conformity with Union law, inform the authority issuing the order of the effect given to the orders, without undue delay, specifying the action taken and the moment when the action was taken. Online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content. Online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the processing of notices and complaints submitted through the notice and action mechanisms and internal complaints-handling systems referred to in Articles 14 and 17 of the

			DSA, respectively, by individuals or entities or by complainants that frequently submit notices or complaints that are manifestly unfounded.
Right of appeal	An effective complaints and redress mechanism available to users of their services in the event of disputes concerning the blocking of access to or removal of original works of authorship or other copyrighted items	Establishing and operating systems through which video-sharing platform providers explain to users of video-sharing platforms what effect has been given to the reporting and flagging. Establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints to the video-sharing platform provider in relation to the implementation of the measures referred to in points (d) to (h) of Article 28b(3) of Directive 2010/13/UE. Member States shall ensure that out-of-court redress mechanisms are available for the settlement of disputes between users and video-sharing platform providers relating to the application of Article 28b (1) and (3) of Directive 2010/13/EU. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law. Member States shall ensure that users can assert their rights before a court in relation to video-sharing platform providers pursuant to Article 28b (1)	Online platforms shall provide recipients of the service, for a period of at least six months following the decision referred to in this paragraph, access to an effective internal complaint-handling system, which enables complaints to be lodged electronically and free of charge, against the following decisions taken by the online platform on the grounds that the information provided by the recipients is illegal content or incompatible with its terms and conditions: a) decisions to remove or disable access to the information; b) decisions to suspend or terminate the provision of the service, in whole or in part, to the recipients; c) decisions to suspend or terminate the recipients' account. Recipients of the service addressed by the decisions referred to in Article 17(1) of the Digital Services Act shall be entitled to select any out-of-court dispute that has been certified in accordance with Article 18(2) of the Digital Services Act in order to resolve disputes relating to those decisions, including complaints that

		and (3) of Directive 2010/13/EU.	could not be resolved by means of the internal complaint-handling system referred to in that Article. Online platforms shall engage, in good faith, with the body selected with a view to resolving the dispute and shall be bound by the decision taken by the body.

Source: the author.

11 Summary

The examples presented above prove the principle that, in each case, the liability of each entity is different, depending on whether it provides the services referred to in the Act on the Provision of Services by Electronic Means, or whether it is a broadcaster or a publisher. As a result of technological and economic convergence, the same entity may perform very different functions, and it is not determined what its status will be, so the scope of its liability is not conclusively determined. The situation calls for appropriate regulations, with the reservation that there is a need to synchronise issues at each stage of legislative activity. It is an element indispensable to creating a coherent system of legislative frameworks facilitating the growth of the digital-services sector, taking into account the basic principles of liability for distributing content. The notice and take-down procedure is still applied in many countries. Directive 2000/31/EC on Electronic Commerce also stipulates that service providers are obligated to respond to content inconsistent with the law, having received a notice (complaint) about the fact. (For more information about digital content-related crime, see K. Chałubińska-Jentkiewicz, 2019:283, especially the chapter on cybercrime [Cyberprzestępczość, wybrane zagadnienia]). Of great importance for the appropriate and effective operation of the notification procedure are special websites appointed for such purpose, by means of which end users may report any illegal content they come across on the internet (Siwicki, 2011:258 et seq.).

Under the present conditions of digital platform development, one expects that the intermediaries of online services should be held to account for content and to protect users, especially those whose rights are being infringed, against certain kinds of illegal content available online. In response to those concerns, in order to ensure greater certainty in the law, and to prevent the fragmentation of the internal market, one needs to consider introducing a framework for reporting mechanisms and removing illegal content (the notice and action procedure) in the territory of the whole EU, covering measures proportional to the character and impact of the mechanisms of damage, to make it possible for unambiguously illegal content to be promptly and effectively removed. The aim is to

minimise potential damage, and to provide a mechanism for securing removed content, if necessary, to prevent, detect, or conduct an investigation in connection with a crime, and to prosecute cybercrime.

It will be necessary, however, to ensure the right balance between the interests and expectations of those who report illegal content which should be removed and those who publish content, making it possible for them to object to its removal (counter-notice). A new regulation must guarantee for the intermediaries of internet services an appropriate level of legal certainty, and improve coordination and cooperation among national authorities and with the European Commission. However, the most important are the interests of network users, the recipients of digital services, who need transparency and a quick reaction. One may not, at the same time, reject internet users' rights to free speech and the right to information.

Another issue worth considering is the character of global competition and respect for consumers' rights. The rigorous rules of competition and open markets have made the EU one of the richest and most competitive economies in the world. The European Commission said that it "is presently analysing the effectiveness of the way in which the relevant provisions of law are applied, for example, to the measures of the protection of competition, and is also evaluating and reviewing these very provisions in order to ensure that they fulfil their objectives in view of the current challenges posed by digital technologies and environmental protection" (Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Shaping Europe's digital future, COM(2020) 67 final, point 2B). Certainly, new provisions are necessary so that they can be adapted to the new conditions of the digital environment. On the one hand, legal provisions which are too rigorous are not conducive to the growth of the market, which creates the risk of evading regulations and registering one's activities in a territory which is less legally restrictive. On the other hand, regulation is required in the case of risks in which only a legal norm is capable of ensuring the socially expected protection of an individual and the state.

References:

Barta, J. & Markiewicz, R. (1998) *Internet a prawo* (Kraków: Wydawnictwo Universitas).

Chałubińska-Jentkiewicz, K., Nowikowska, M. & Wąsowski, K. (2020) *Media w erze cyfrowej. Wyzwania i zagrożenia* (Warszawa: Wolters Kluwer).

Chałubińska-Jentkiewicz, K. (2019) *Cyberodpowiedzialność* (Toruń: Wydawnictwo Adam Marszałek).

Garton Ash, T. (2018) *Wolne słowo. Dziesięć zasad dla połączonego świata* (Kraków: Wydawnictwo Znak).

Gęsicka, D.K. (2014) *Wyłączenie odpowiedzialności cywilnoprawnej dostawców usług sieciowych za treści użytkowników* (Warszawa: Wolters Kluwer).

Gołaczyński, J. (ed.) (2009) *Ustawa o świadczenie usług drogą elektroniczną* (Warszawa: Woleters Kluwer).

Konarski, X (2020) Nowe obowiązki dostawców usług internetowych w prawie polskim i Unii Europejskiej, *Monitor Prawniczy*, 2020(20), pp. 147 - 153.

Litwiński, P. (2004) Świadczenie usług drogą elektroniczną, In: Podrecki, P. (ed.) *Prawo Internetu* (Warszawa: Wydawnictwo Prawnicze LexisNexis), pp. 166-245.

Markiewicz, R. (2021) *Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790* (Warszawa: Wolters Kluwer).

Rączka, G. (2009) Prawne zagadnienia hostingu, *Przegląd Prawa Handlowego*, 2009(4), pp. 31-37.

Siwicki, M. (2011) *Nielegalna i szkodliwa treść w internecie* (Warszawa: Wolters Kluwer).

Spindler, G. (2019) The Liability system of ART. 17 DSMD and national implementation – contravening prohibition of general monitoring duties, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10(3), pp. 344-374.

Woźniak, M. (2019) Antykonkurencyjne praktyki w relacjach między przedsiębiorcami: uwagi na tle nowego rozporządzenia P2B, *Zeszyt Naukowy.pl. Wyższa Szkoła Zarządzania i Bankowości w Krakowie,* (52), pp. 1-10.

Zieliński, M. (2013) *Odpowiedzialność deliktowa pośredniczących dostawców internetowych. Analiza prawno porównawcza* (Warszawa: Wolters Kluwer).

The Role of the State and Public Administration in the Cybersecurity System

TOMASZ ZDZIKOT

Abstract Following the guidelines of satisfying collective needs and acting by the administration in the public interest, it should be pointed out that security is one of the most important individual and collective needs. Ensuring cybersecurity is, therefore, one of the state's tasks carried out with the help of public administration to meet the collective and individual need for security. There is no doubt that in order to perform its tasks effectively in a changing security environment and to meet new challenges, public administration must undergo a series of structural and functional transformations. The state is obliged to ensure appropriate organisational, human and technical resources, which are necessary for the implementation of tasks. The objective awareness of threats and international obligations, and national legal regulations, as well as strategic documents, require far-reaching commitment in this respect.

Keywords: • public administration • cybersecurity • strategy

CORRESPONDENCE ADDRESS: Tomasz Zdzikot, President of the Management Board of Poczta Polska SA, Ul. Rodziny Hiszpańskich 8, 00-940 Warszawa, Poland, e-mail: tomasz@zdzikot.pl.

https://doi.org/10.4335/2022.2.2 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Public objectives and tasks

The doctrine of law distinguishes three basic meanings of the term "administration", among which the first one assumes, as the basic determinant, the organisational structures set up in the state to pursue public task objectives, the second refers to the activities conducted with a view to accomplishing public task objectives, while the third takes into account people employed in organisational structures (Boć, 2010: 12).

The terms "public purpose", "public task" and "public interest" are indeterminate and changeable, depending on the political and social conditions, legal contexts, as well as the system of values accepted as the basis for the functioning of administration in a given time and place. Appearing in lower- and higher-level legal acts, constitutional acts, and substantive and procedural acts, the terms in question play a special role and are most often interpreted as determinants of the permissible scope of interference in the sphere of rights of the an individual and his/her personal interests. The terms "public purpose" and "public interest" have not been defined in a universal way, which results from their nature being relativised subject to changeable external conditions. Hence, the Polish Constitution not only lacks a definition of public purpose, but also does not specify any circumstances under which particular purposes could be deemed public. According to the Polish Constitutional Tribunal, "Whatever serves the commonalty, is generally available or represents the interest of the whole society or regional community, can be deemed public purpose" (Constitutional Tribunal, 2015).

The doctrine emphasises that the meaning of the term "public purpose", as determined on the basis of the above guidelines, may not be subject to extensive interpretation, while its scope may cover only the most common categories of matters connected with satisfying the needs of the population. Deliberations on the essence of public purpose thereby coincide with the category of public tasks. The term "public task" is also deemed indeterminate although tasks are always determined on the basis of binding legal norms. As it has already been mentioned, public tasks are defined by public purposes which public administrations are obliged to meet, whilst the purposes are associated with the public interest. The doctrine points out that the public character of a task means, on the one hand, that it has a normative basis and that, in carrying it out, the state (local government) acts in the public interest – for the common good, construed as certain basic values of a given community. Simultaneously, assigning to a specific task the quality of a public task will imply the recognition that their performance belongs to the duties and not to the powers of public authorities (Strożek-Kucharska, 2016: 122-123). In this approach, public tasks are, first and foremost, constitutional duties of state (local government) authorities, the scope of which cannot be unilaterally limited for political or economic reasons, nor can the state (local government) derogate from their performance, since the raison d'être of the state (local government) is precisely to take specific actions in the collective interest (Blaś, 2003:144).

There is no list or time-invariant set of tasks that, by their very nature, have the permanence of the quality of public tasks. However, some authors perceive a sphere of public tasks which are characteristic for the operation of the state and which can be defined as "model" tasks or public tasks in their pure form. These include in particular ensuring external security and internal order, i.e., those tasks whose performance requires coercion.

The term "public task", as well as the terms "public purpose" and "public interest", are commonly interpreted as limiting the scope of legally permissible activity of a public entity. At the same time, it is assumed that satisfying community needs will always have the nature of a public task, which has been confirmed by the Constitutional Tribunal by indicating that public tasks comprise all tasks of the local government, as they aim at satisfying collective needs (Bandarzewski, 2007: 331-332, Constitutional Tribunal, 1994)

2 Ensuring cybersecurity as a task of the state and the administration

Following the guidelines of satisfying collective needs and acting by the administration in the public interest, it should be pointed out that security is one of the most important individual and collective needs. Ensuring security was, historically speaking, one of the basic factors determining the creation of communities, from neighbourhoods, families and tribes, to the state as the most perfect form of ensuring security for individuals and social groups. Viewing the state through the prism of its functions, construed as the course of action, it is recognized that ensuring internal and external security is of primary importance among them (Czuryk, Dunaj, Karpiuk and Prokop, 2016: 17,19). Security is thus clearly one of the basic values to which constitutional norms refer by distinguishing many of its categories, including security of citizens, security of the state, and internal and external security.

The literature emphasises that the purposes and functions of the state are not identical concepts although they remain closely related. This is a primary purpose in relation to the function, which is instrumental in relation to the intended purpose. Since the state is a purpose-driven institution, the question about the purposes of the state is in fact a question about the essence of the state, about why the state exists and what society wants to achieve through this form of organisation. The purpose will, therefore, be the object of the intended action, the indicated state of affairs pursued by the state, what it wants to achieve and meet, while the function will be the course of action of the state that serves to achieve and meet the intended purpose (Safjan, Bosek, 2016). The relation between purposes and tasks is similar, whereby it is noted that both purposes and tasks are closely related to the category of values realised by public administration. In the case of tasks, it is a time-specific assessment of a present state that is being pursued, an object, a fact or an event, in relation to the lawmaker's system of values, while in relation to the purpose it will be an identical assessment of a projected future state (Cieślak, Bukowska, Federczyk Klimaszewski, Majchrzak, 2012: 14).

From the afore-described point of view, it is more appropriate to consider security as a general purpose of the state being pursued through the performance of a number of tasks. As already mentioned, security is one of the most important values for every human being. In the classic A. H. Maslow's pyramid, which defines the hierarchy of needs, security takes the second place, after physiological needs, and before belonging, esteem and self-actualisation. Considering the foregoing, the doctrine rightly states that the role of the state, and consequently the role of public administration, is to organise social life in such a way so that the need for security could be satisfied both in the subjective dimension (where in the narrow sense it applies to a person, and in the broad sense it applies to the society and the state) and in the objective dimension (involving specific types of security, i.e., for example, energy, financial or transport security) (Czochowski, 2014: 274-275). Cybersecurity must also be considered in this sense. In terms of the object, it covers an increasingly broad spectrum related to the creation of "cyberspace" aggregating hardware, software, networks, systems and human activity in this environment, while in terms of the subject, in connection with the ongoing processes of digitisation, cybersecurity threats may harm both individuals and communities as well as organisations or, finally, states. Hence, it is reasonable to treat cybersecurity (ICT security) as common welfare, leading to the necessity to "create a special legal protection system, under which certain obligations must be assigned to public administration authorities performing regulatory functions and to telecommunication entrepreneurs, while ICT security itself should be subject to either criminal or criminal and administrative legal protection – depending on the gravity of the action affecting it". (Czyżak, 2014: 288).

3 Obligations of NATO Allies

Given the framework of this study and the breadth of the issue at hand, the international implications will be discussed in the outline referring to the most relevant issues of topical nature. From the perspective of the involvement of the state and public administration in cybersecurity efforts, the decisions made in 2016 were crucial in the international arena.

Firstly, cybersecurity issues were among the leading issues at the NATO Summit held in Warsaw on 8-9 July 2016. In the final declaration of the Summit, the heads of the Allies stated that they had committed to "to enhance the cyber defences of our national networks and infrastructures, as a matter of priority" (NATO, 2016a). Simultaneously, NATO expected that "Each Ally will honour its responsibility to improve its resilience and ability to respond quickly and effectively to cyber attacks, including in hybrid contexts". (NATO, 2016a) The theses formulated in the final declaration were developed in the Cyber Defence Pledge, also adopted at the Summit (NATO, 2016b). In this document, in recognition of the new realities of the security threats to NATO, the Heads of State and Government pledged to ensure that the Alliance keeps pace with the rapidly evolving cyber threat landscape and that NATO nations will be capable of defending themselves in cyberspace as in the air, on land and at sea. They also reaffirmed their national

responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and their commitment to the indivisibility of Allied security and collective defence. The Cyber Defence Pledge also lists seven specific commitments which the Allies are required to fulfil:

I. Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks;
II. Allocate adequate resources nationally to strengthen our cyber defence capabilities;
III. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices;
IV. Improve our understanding of cyber threats, including the sharing of information and assessments;
V. Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;
VI. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;
VII. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends (NATO, 2016b)

To ensure that the commitments outlined in the Cyber Defence Pledge would not become an empty declaration, a monitoring system was also envisaged. Thus, it was agreed that progress on the fulfilment of the commitments would be tracked and reviewed on an annual basis. A detailed questionnaire was created for this purpose, on the basis of which the Allied states carry out self-assessment, taking into account the changes in individual countries, including, for example, organisational, structural or legal changes. NATO may also ask additional questions in the area of interest (the so-called Focus Area). On the basis of the data collected this way, enriched with information obtained during bilateral meetings, a report is created containing an assessment of the fulfilment of the commitments included in the Cyber Defence Pledge, which is presented annually during meetings of NATO defence ministers. The report takes into account, among other things, weaknesses and recommendations, and each Allied state receives individual feedback from NATO.

4 Obligations of EU Member States

Additionally in 2016, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, referred to as the NIS Directive, was adopted. The essence of the regulation was to oblige all European Union Member States to guarantee a minimum level of national capabilities in the area of ICT security. The

provisions of the directive revolve around three pillars: institutions, European cooperation and obligations in the field of network and information security (Wrzosek, 2016). In the first area especially, although not only, the obligations of Member States to act in the sphere of cybersecurity are emphasised. EU Member States have thus been obliged to:

- designate at least one national competent authority on the security of network and information systems (also from among the existing authorities), whose primary task is to monitor the application of the Directive at the national level, by means of a set of minimum powers which the Directive requires competent authorities to have at the national level,
- designate a national single point of contact on the security of network and information systems (also from among the existing authorities), which will exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States, and with the Cooperation Group and the CSIRT network set up under the Directive,
- designate at least one Computer Security Incident Response Team (CSIRTs), comply with the requirements set out in the Annex to the Directive, which will be responsible for risk and incident handling in accordance with a well-defined process, at least for the digital sectors and services described in the Directive,
- develop and adopt a national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented.

Importantly, the Directive contains several obligations for Member States to provide the necessary tools and resources, especially to the competent authorities, the single points of contact and CSIRTs to ensure that they carry out, in an effective and efficient manner, the tasks assigned to them, and thereby to fulfil the objectives of this Directive. It should be highlighted that technical, financial and human resources are indicated explicitly.

It is also worth noting at this point that on 16 December 2020 the European Commission presented, *inter alia*, a proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – being a revised version of the NIS Directive, i.e., the so-called NIS Directive 2 (European Commission, 2020). What draws attention to the catalogue of proposed changes is, *inter alia*, the extension of the subjective scope of the Directive to sectors not previously covered by the NIS Directive. The NIS 2 project takes into account two types of entities: essential entities and important entities. Especially with regard to the latter, the change is noticeable. From among the six sectors in which important entities should operate, only digital providers have been included in the scope of the Directive. The scope of obligations imposed by the NIS 2 Directive on both essential and important entities will also increase significantly. Among the numerous obligations, it indicates, inter alia, the need to ensure supply chain security. Great importance is also attached to certification. The proposal assumes that Member States may require essential and important entities to certify certain products, services and processes under specific European cybersecurity certification schemes provided for in the Cybersecurity Act.

The above changes are closely linked to a significant extension of the tasks of national authorities competent for cybersecurity, which are to exercise supervision over essential and important entities. This, in turn, will mean that national cybersecurity structures will have to be built more dynamically and that EU Member States will have to ensure an adequate level of funding for the tasks imposed on public administration. As experts note, the new tasks will require large resources on the part of public administration, while the sectoral approach to supervision adopted in Poland, combined with the obligation to establish sectoral CSIRTs, will necessitate the allocation of significant funds for this purpose within the state budget (Wrzosek, 2020).

5 Polish solutions in outline

In Poland, the NIS Directive was implemented by way of the Act of 5 July 2018 on the National Cybersecurity System. As indicated in the explanatory memorandum to the proposal for this Act, the comprehensive regulation of the national cybersecurity system results "on the one hand, from the need to ensure a systemic approach to the national cybersecurity system in the face of constantly growing and dynamically changing threats to the operation of the state, economy and society, and, on the other hand, from the need to implement Directive 2016/1148 into the Polish legal order" (Council of Ministers, 2018).

The scope of action of the state and its administration is, therefore, defined in Poland in:

- national legislation of various rank – from the Constitution, through the Act on government administration departments, to the Act on the National Cybersecurity System, which, as mentioned above, implements the provisions of the NIS Directive, together with the implementing acts,
- strategic documents, including in particular the "Cybersecurity Strategy of the Republic of Poland for 2019-2024", which was approved by the Council of Ministers on 22 October 2019 and signed by the Prime Minister on 29 October, effective from 31 October 2019. The strategy superseded the previous "National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022",
- international agreements and commitments, such as the afore-described NATO Cyber Defence Pledge.

The national cybersecurity system that has been shaped and developed in Poland is decentralised. The performance of tasks in this area belongs to many entities, and their effectiveness depends on the cooperation of the units and individuals involved (Zdzikot, 2018: 249).

Pursuant to Article 146 (4), (7), (8) and (11) of the Constitution of the Republic of Poland, the Council of Ministers is responsible for ensuring the internal and external security of the state, as well as public order, and exercises general control in the field of national

defence. The basic divisions within the Council of Ministers was introduced by the Act of 4 September 1997 on government administration departments, which preordains that cyberspace security in the civilian dimension belongs to the department of "computerisation", which is today headed by the President of the Council of Ministers, while historically it was under the competence of the Minister of Digitalisation (whose ministry is currently not a separate department within the government), whilst cyberspace security in the military dimension is part of the department of "national defence", headed by the Minister of National Defence.

Under the Act on the National Cybersecurity System, in the above-described underlying issues resulting from the NIS Directive, the following solutions were introduced into the Polish system:

- with regard to the designation of competent authorities for network and information systems security, the regulatory model adopted in the Act provides for an extension of the competences of sectoral authorities in the field of cybersecurity, instead of establishing a single national cybersecurity authority at the central level. Responsibilities of an administrative, regulatory and control nature have been assigned to ministers competent for the sectors listed in the NIS Directive;
- the operation of the Single Point of Contact is the responsibility of the minister in charge of computerisation;
- in accordance with the requirements set out in the NIS Directive, three Computer Security Incident Response Teams have been established, headed by the Minister of National Defence (CSIRT MON), the Head of the Internal Security Agency (CSIRT GOV) and by the Research and Academic Computer Network - National Research Institute (CSIRT NASK);
- the "Cybersecurity Strategy of the Republic of Poland for 2019-2024" is being implemented, the main objective of which is "to increase the level of resilience to cyber threats, as well as the level of information protection in the public, military and private sectors and to promote knowledge and good practices to enable citizens to better protect their information".

As already mentioned, apart from legal regulations, strategic documents also, or perhaps especially, reflect the way the state perceives its role in the area of cybersecurity, as well as the directions of intervention, which with the help of the administration will be applied to achieve the objectives. The Polish Strategy for 2019-2024 identifies five specific objectives:

1) Developing a national cybersecurity system;
2) Increasing the level of resilience of information systems of the public administration and the private sector, and achieving the capacity to effectively prevent and respond to incidents;
3) Increasing the national capacity in the area of cybersecurity technology;
4) Building public awareness and competences in the area of cybersecurity;
5) Building a strong international position of the Republic of Poland in the area of cybersecurity.

Within the framework of the National Cybersecurity Strategy, the Ministry of Defence has also implemented its own programme since 2019, which fits in with and complements it, and which has identified, within a wide-ranging programme called CYBER.MIL.PL, four core areas of activity:

1) the consolidation and building of cybersecurity structures,
2) education, training and coaching,
3) cooperation and building a strong international position, and
4) increasing the level of security of ministerial and military networks and systems (Complete information including summaries of the individual stages of implementation is available at www.cyber.mil.pl).

6 Summary

Ensuring cybersecurity is, therefore, one of the state's tasks carried out with the help of public administration to meet the collective and individual need for security. There is no doubt that in order to perform its tasks effectively in a changing security environment and to meet new challenges, public administration must undergo a series of structural and functional transformations. The first widely commented and described digital attacks on critical infrastructure date back to the mid-1990's (for example, in 1997, an attacker disabled telephone lines at the Worcester Airport (USA), which were used by the control tower, the airport security services, the airport fire brigade, and the weather service. The runway lighting system was also disabled). Today, the activities of the state and public administration aiming at ensuring cyberspace security are forced not only by the general awareness of threats, but also by international, Union and national legal regulations and strategic documents.

At the same time, ensuring security in cyberspace, in its individual and collective dimension, is a cross-cutting task, the implementation of which rests with a number of authorities and units, especially bearing in mind that the national cybersecurity system constructed by the Polish legislator is not centralised.

In view of the above, the tasks of the state and public administration include, in particular, constructing appropriate mechanisms, processes and procedures for the whole system to ensure, and to continuously improve, the level of cybersecurity against any changing threats. The specificity of this area means that not only command and control powers, but also those from the sphere of dominion, play an important role. The state is obliged to ensure appropriate organisational, human and technical resources, which are necessary for the implementation of tasks. The objective awareness of threats and international obligations, and national legal regulations, as well as strategic documents, require far-reaching commitment in this respect.

References:

Bandarzewski, K. (2007) Prywatyzacja zadań publicznych, In: Zimmermann, J. (ed.) *Koncepcja systemu prawa administracyjnego* (Warszawa: Wolters Kluwer Polska), pp. 331-345.

Błaś, A. (2003) Zadania administracji publicznej. Zadania administracji publicznej w państwie prawa, In: Błaś, A., Boć, J. & Jeżewski, J. (eds.) *Administracja publiczna* (Wrocław: Kolonia Limited), pp. 139-144.

Boć, J. (ed.) (2010) *Prawo administracyjne* (Wrocław: Kolonia Limited).

Chochowski, K. (2014) Bezpieczeństwo publiczne jako dobro publiczne, In: Woźniak, M. & Pierzchała, E. (eds.) *Dobra publiczne w administracji* (Toruń: Adam Marszałek), pp. 265-279.

Cieślak, Z. (ed.), Bukowska, J., Federczyk, W., Klimaszewski, M. & Majchrzak, B. (2012) *Nauka administracji* (Warszawa: LexisNexis).

Czuryk, M., Dunaj, K., Karpiuk, M. & Prokop, K. (2016) *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne* (Olsztyn: WPiA UWM).

Czyżak, M. (2014) Bezpieczeństwo teleinformatyczne jako dobro publiczne i wybrane aspekty jego prawnej ochrony, In: Woźniak, M. & Pierzchała, E. (eds.) *Dobra publiczne w administracji* (Toruń: Adam Marszałek), pp. 286-298.

NATO (2016a) *Deklaracja końcowa szczytu NATO w Warszawie Wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r.*, available at: https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (August 30, 2022).

Safjan, M. & Bosek, L. (eds.) (2016) *Konstytucja RP. Tom I. Komentarz do art. 1–86* (Warszawa: C.H. Beck).

Strożek-Kucharska, M. (2016) Definiowanie zadań publicznych – wprowadzenie do dyskusji, In: Bieś-Srokosz, P. (ed.) *Zadania publiczne. Podmioty-uwarunkowania prawne-potrzeby społeczne* (Częstochowa: Wydawnictwo im. S. Podobińskiego, Akademii im. Jana Długosza w Częstochowie).

Wrzosek, M. (2016) *Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństwa* (NASK), available at: https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/ (August 30, 2022).

Wrzosek, M. (2020) *Dyrektywa NIS 2 – jakie zmiany w zakresie cyberbezpieczeństwa proponuje Komisja Europejska?* (NASK), avalable at: https://cyberpolicy.nask.pl/dyrektywa-nis-2-jakie-zmiany-w-zakresie-cyberbezpieczenstwa-proponuje-komisja-europejska/ (August 30, 2022).

Zdzikot, T. (2018) Państwo i administracja publiczna na straży cyberbezpieczeństwa, In: Federczyk, W. (ed.) *Stulecie polskiej administracji. Doświadczenia i perspektywy* (Warszawa: Krajowa Szkoła Administracji Publicznej im. Prezydenta Rzeczypospolitej Polskiej Lecha Kaczyńskiego).

The Role of Network Technologies in European Cybersecurity

URSZULA SOLER

Abstract The twentieth-century technological revolution changed nearly all spheres of human life. The changes are particularly evident in the domain of communication where network technologies (the internet, satellite communication, etc.), which accelerated the development of social communication in an unprecedented way by eliminating and marginalising the significance of geographical, political or cultural borders, have played a pivotal role. However, the need for their social assessment is being raised increasingly because, on the one hand, network technologies serve the daily lives of millions of people very well, whereas, on the other hand, by analogy, they are accessible to socially detrimental groups, e.g., terrorists, enabling them to perform extremely hostile activities. So, may their social assessment be unambiguous? Many research centres dealing mainly with tracking, analysing and assessing terrorist acts committed by various groups all over the world are emerging in the United States and Europe. Network technologies are, among other things, utilised to commit these acts and to track them. This paper is devoted to the social assessment of the role played by network technologies in European cybersecurity.

Keywords: • network technologies • modern technologies • terrorism • society • technology rating • technology assessment

CORRESPONDENCE ADDRESS: Urszula Soler, Ph.D., Associate Professor, The John Paul II Catholic University of Lublin, Social Sciencies Faculty, Al. Racławickie 14, 20-950 Lublin, Poland, e-mail: urszula.soler@gmail.com.

https://doi.org/10.4335/2022.2.3 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Twentieth-century technological changes influenced the development of industry and services, but most of all, modified human communication in an unprecedented way. For less than one hundred years, the speed of communication have multiplied to an extent that spatial distances are no longer important. The foundation of international companies employing people from different countries who "meet" and work with the use of modern communication technologies has become the standard of the 21st century. The tendency was accelerated yet again over the last two years by the outburst of the COVID-19 pandemic. Network technologies are technologies that, in the recent decades, have brought about a special revolution, also covering the social dimension. Their emergence and development have uniquely impacted social life bringing with them numerous alterations, not only to the domain of communication, but also to threats. Their potential is utilised by ordinary people, governments, non-governmental organisations or the world of business. However, it rapidly transpired that network technologies are not only a great social asset but may be detrimental to society too. Socially detrimental groups – the world of crime or broadly speaking, international terrorism – very quickly started to utilise these technologies due to having unlimited access to them. This article is dedicated to the social assessment of the role played by network technologies in cybersecurity in Europe and whether, in the background of terrorist attacks, the rating of network technologies may be socially unambiguous. The method applied in this article is based on the analysis of existing literature and network studies carried out by European cyberterrorism research organisations.

2 Theoretical aspects – definitions

The most important terms concerning network communication and terrorism, which also utilises communication, are defined in this subchapter.

The term *network technologies* appeared for the first time at the end of the 1990s due to the development of the communication potential of the internet. The emergence of the internet, in combination with new achievements in telecommunication and computer sciences, lead to another great technological transformation – a shift from dispersed, isolated microcomputers and supercomputers to wide informatisation by means of interconnected information-processing devices utilising various formats (Castells, 2007:63). As time went by, computer devices penetrated all possible spheres of life and activity: home, work, stores, entertainment, transport, etc. The devices, often mobile ones, were able to communicate with each other without using their operating systems. The basic technology, applications and data are stored on network servers and the computational intelligence is embedded in the network itself: the sites communicate with each other and utilise necessary software enabling them to connect any device to a universal computer network. The network logic embodied by the internet started to be applied in each domain of activity, each context and each electronically connectable place (The Economist, 1997).

Network technologies are often called information-communication technologies or ICTs. This is a wide concept encompassing all technical means used for the transmission of information. In other words, ICT corresponds to the application of digital technologies that help people to process and transmit information. The technologies have a large array of applications – from personal computers to PDAs (Personal Digital Assistant), from mobile to satellite phones or from faxes to robots. The demand for more advanced communication technologies lead to extensive development in the late 1970s. At that time, telecommunication engineers dreamt about one thing – the death of distance (Cairncross, 1997:118). Over time, the dream became a reality and technologies such as the internet or satellite phones have emerged.

Modern technology-based communication changed ordinary human lives to an extreme degree. It is said nowadays that we are living in a global village where information serves all. All of it happened due to the information and communication revolution. Information and communication technologies have definitely changed peoples' lives. People utilise them in social communication, education or business. Collaborative virtual environments (CVE) gave business people a lot of opportunities to expand their activities all over the world – in various geographical locations – and, at the same time, enabled them to maintain their headquarters in their natural place of work and life. Satellite telephones diminished the distance in interpersonal relations. Relationships among people living in different cities, countries, sometimes even continents, have become quite common and are no longer surprising for anybody. The dream of twentieth-century engineers about the death of distance became true, and the outburst of SARS-CoV-2 additionally accelerated or even forced the death of communication distance.

Terrorism and its younger sibling – cyberterrorism – are among the most controversial terms in the modern world. There is not one, universally accepted definition of terrorism, with governments of different countries and agencies fighting terrorism using their own definitions of terrorism. According to a study carried out in 2003 by Jeffrey Record from the US Army, there are over 100 definitions of terrorism. Their range encompasses 22 different definition elements in total (Record, 2003). The term became controversial due to the mixing of interests of various states and nations. The problem is reported, among others, by the United Nations Organisation. However, due to the conflict of interests among sovereign states that each time individually define which entity is a terrorist and which is a freedom-fighter, the Organisation is not able to decide on the definition of terrorism (Koechler). It often happens that in one state a person is considered a freedom fighter and a terrorist in another.

According to Todd Sandler and Walter Enders, terrorism is the threat of using violence or the premeditated use of violence by people or national groups to achieve political and social goals by intimidating a large group of recipients with direct victims (Sandler, Enders). According to the researchers, there are two basic components characterising each modern definition: the presence or the threat of violence and a political/societal

motive. Without violence or the threat of using it, terrorists are not able to influence political decisions made in response to their demands, and if a political/societal motive is missing, the act of violence is a crime and not an act of terrorism (Sandler, Enders). Yet another, simplified definition of terrorism is approved by the National Consortium for the Study of Terrorism and Responses to Terrorism – START at the U.S. Department of State. From their perspective, terrorism is the threat of using or the actual use of illegal force by non-state actors to achieve a political, economic, religious or social goal through fear, coercion or intimidation (the International Institute for Counter-Terrorism).

Cyberterrorism is a younger sibling of terrorism that appeared with the emergence of network technologies. Simply put, it is a marriage between technology and terrorism. This type of terrorism is directly linked to technological progress. The term itself was introduced following the rapid and uncontrolled development of technology. The term *cyberterrorism* is equally controversial as the term *terrorism* and there is not one universal definition of it. Some scientists argue that the use of computers or resources of information technologies to commit any act of terrorism justifies the use of the term *cyberterrorism*. Others claim that cyberterrorism is an abuse of information systems and databases, e.g., the hacking of databases of organisations and obtaining information for illegal purposes. One of the definitions is cited by Dorothy E. Denning. In her opinion, it is a convergence between terrorism and cyberspace. These are generally understood as illegal attacks or the threats of attacks on computers, networks and information stored there in order to intimidate or force a government or people to act upon demands and to achieve specific political or societal goals. Moreover, to classify an attack as cyberterrorism, it needs to be violent towards people or property or at least cause fearful damage. Therefore, these are attacks leading to death or injury, explosions, plane crashes, water pollution or serious economic losses. Heavy attacks on key infrastructure may or may not be acts of cyberterrorism, depending on their size and impact. Attacks disrupting insignificant services or burdensome in financial terms are not acts of cyberterrorism (Denning, 2000).

There is yet another term associated with cyberterrorism, i.e., *pure cyberterrorism*. It is also sometimes called *bloodless terrorism*. It refers to acts of terrorism that only happen in the virtual world. Bank intrusions are an example of this. Terrorist organisations need funds to conduct their activities in the real world, and thanks to modern online banking systems and the full set of internet financial services, they are able (through cyberterrorism) to steal money from banks and then use it to finance other terrorist activities. The idea was discussed in 1991 and presented in the report titled "Computers at Risk" prepared by the Board of the American Computer Science and Telecommunications. The authors of the report pointed to the danger resulting from the fact that state functioning is too highly dependent on computers. Computers control energy supplies, air communication and financial services. They are utilised to store important information, medical registries, penal registries, and are also used by business. And despite common social trust, they are exposed to terrorist attacks due to improper construction and insufficient quality control mechanisms. A modern thief is able to steal

more money using a computer than a pistol. According to these authors, a terrorist of the future may cause more harm using a keyboard than a bomb (the National Research Council, 1991). Unfortunately, these predictions have already turned out to be true.

3 Can the development of network technologies prove socially detrimental?

In this paragraph, the social usefulness, and potentially detrimental effects, of network technologies are discussed on the basis of examples of specific technologies.

By assumption, new technologies are always supposed to serve the greater good of society and people, but due to the lack of limitations and easy access, there is no guarantee that the technologies are always used in accordance with their intended purpose. Google Earth technology (a computer programme displaying satellite, aerial and panoramic images taken from street level, as well as various types of geographical and tourism information on a three-dimensional model of the globe), is one of many modern technologies utilised by scientists from various disciplines, which serves as an example. It is used, among other things, to create maps for measuring the susceptibility of the earth's surface to floods and earthquakes or other natural disasters. At the same time, however, the technology may also be used for killing hundreds of innocent people. An example is the use of it by terrorists involved in attacks in Mumbai, India in 2008 (The Washington Post).

Biometric tools, utilised mostly to control the access to protected premises or authorised users accessing specific data, programmes or devices (unauthorised attempts to access ATMs, personal computers, computer networks, mobile phones, home alarm systems, etc.) are socially useful and one of the most dynamically developing areas of telecommunication and information technologies. Some countries implemented biometric solutions for border control. They are successfully used, for instance, in airports in the United States and Australia. Australia decided to implement the *Smart Gate* face recognition system (Gamm, Sester, Reindl, 2013:45-50) operating in parallel with traditional points of passport control. Passport control with the use of a face reading device lasts only 6 seconds. France (face recognition) and Great Britain (human iris identification) also intend to implement biometric systems. The spread of the Wuhan virus has rapidly accelerated the development of biometric technologies. At the same time, however, terrorists improve the methods of passing by or falsifying the biometry (it is suffice to mention money counterfeiting).

Visual Surveillance – namely, the monitoring of behaviour and the habits of people to influence, direct and protect them (Lyon, 2007) is yet another example of network technologies. It may encompass distant observation by means of electronic devices (such as CCTV cameras) or capturing information sent via an electronic route (such as the internet or phone) (Minsky, Kurzweil, Mann, 2013:13-17). The system is utilised by governments for intelligence purposes, combating crime, the protection of processes, people, groups and crime investigation, to name a few. It is also used by criminal organisations for planning and committing crimes such as assaults or abductions.

Tracking of personal data, namely, obtaining personal information from various sources, comparing them and drawing up subsequent conclusions based on them in order to create a profile with the use of modern communication tools, is often utilised nowadays. The use of large sets of data may be very advantageous for businesses, governments and non-profit organisations. However, it is also stressed that, considering the rules of protection of data and privacy, the phenomenon of profiling should be limited to a necessary minimum. Informing users that they are subjects of profiling, even if it is carried out on the basis of commonly accessible sources, is also highly important. Various types of profiling are used to combat terrorism (Podniesienie skuteczności działań policji, 2010) (profiles based on specific intelligence information, profiles not based on specific intelligence information, profiling by "data exploration"), while it is ethnic profiling that has seen an increase in recent years. (It is nothing new in the Member States of the European Union. Its significance has increased in response to terrorist attacks in the United States (2001), Madrid (2004) and London (2005), and to growing concerns about illegal immigration). However, the use of ethnic profiling also raises concerns among intergovernmental organisations such as UNO, the Council of Europe and the European Union, as well as non-governmental organisations dealing with the protection of human rights. One argument that is cited particularly often is that ethnic profiling not only collides with the law on discrimination but also brings disadvantageous societal effects. In addition, terrorists often utilise false profiles to hide their true identities.

Reconnaissance satellites – often commonly referred to as spy satellites – are yet another, modern network technology. Their goal is to observe objects on the earth and capture signals from the earth for military or intelligence purposes. The observation is often linked with taking high-resolution photographs (up to below 1 m) that may be used in various ways (for example, to track the movement of enemy military troops or obtain information on potential targets on an enemy's territory). There are also satellites capable of obtaining information through clouds and at night, taking infrared photographs or using radar. Their basic goal is to provide data concerning the economic-military potential of a probable opponent, structures and equipment, as well as the location of an opponent's troops and the level of preparation for state defence (Nowacki, 2002:57-64). The Allied Forces operation, carried out by the forces of the North Atlantic Treaty Organisation (NATO) from 24 March and 20 June 1999 in the Federal Republic of Yugoslavia, aimed to put the ethnic cleansing in Kosovo to an end, to restore the multi-ethnic character of the province and to force the process of democratisation in Yugoslavia, is an example of satellite use. Aerial and space reconnaissance means were mostly used (Marszałek, 2009). During the operation, reconnaissance satellites (IMINT, Imagery Intelligence satellites, equipped with electro-optical apparatus and high-resolution infrared sensors (IR), Lacrosse satellites for radar imagining of the operation's area and ELINT/SIGINT satellites of the Mercury, Mentor, Trumpet and Orion type, assigned for capturing electronic signals in a wide range of frequency) mostly tracked the location of Serbian military forces and their communication, capturing radio signals and taking photographs of the enemy's military posts. In theory, satellites may not be used for unlawful purposes,

however, the practice proves otherwise. Like in the case of other technologies, satellites may be utilised by terrorists for the same purposes as military ones.

Computers and the internet are yet another examples of not so recent network technology that, on the one hand, is helping to combat terrorism but, on the other hand, is likely to serve terrorist purposes. Cyberterrorism was mentioned in the preceding paragraph while some more examples are discussed here. Computers were originally designed as computational machines, and in time, they became a medium utilised in nearly all spheres of human life. In combination with the internet (originally designed for the military in the form of the ARPANET network), their capabilities increased incalculably and are utilised for combating crime and terrorism, but also serve terrorism itself. It is suffice to mention bank account intrusion, illegal network transactions, and the Dark Web (Deep Web, Deepnet, Invisible Web, Hidden Web).

The Dark Web (Egan) is the term referring to a specific set of sites that are theoretically visible to all, but their IP addresses and host servers are hidden. It is a huge network of encrypted internet sites inaccessible through ordinary search engines (Wasiuta, 2019:251). To access them, one needs to use specially designed applications. Moreover, a skilful configuration of network settings is needed (Merriam-Webster.com). Nearly all sites of the Dark Web hide their identity using Tor, an encryption tool enabling the end-user to hide their identity and to falsify their location. To enter the Dark Web site encrypted with Tor, Tor needs to be used.

The Dark Web, called "the shady network", is a small proportion of the overall percentage of the Deep Web. The majority of sites encrypted on the Dark Web are typically amateur because it is easy to create a profile and win publicity there. The dark side of the internet is beyond the influence of the largest corporations dealing with technological development or media institutions. The Dark Web is constantly developing and the amount of money generated from transactions performed there remains immeasurable. It is strongly related to the first internet networks, such as ARPANET, due to the fact that both links are universally recognised under their shameful name as "a haven for illegal activities" (Beattie). The complexity of the operating schemes of search engines adjusted to surfing the Dark Web makes the reviewing of content very difficult and chaotic because the addresses of internet domains are almost constantly changing to ensure total non-detectability of their users. At first glance, the majority of sites resemble the ordinary internet that we use daily. However, they are differentiated by the fact that their names do not end with a classic .com or .pl, but with .onion (Stawska). Some people excessively use the Dark Web because anonymity helps them to commit various crimes – from paid killings to child pornography and stealing sensitive data such as personal photographs, medical records encompassing health condition information or documents proving the financial resources of private individuals (Beattie).

According to the Cambridge Dictionary, the Deep Web is "parts of the internet that cannot be found using ordinary search engines" (Cambridge Dictionary). It needs to be noted

that definitions of the Dark Web and Deep Web are similar to each other, but the Dark Web is only a small part isolated from the Deep Web. The size of the Deep Web is immeasurable. The Deep Web contains huge amounts of data and many various sites. The unindexed resources are inaccessible through popular search engines, but indexed sites may also be found there, but access to them is not as easy as in an ordinary internet network. The causes of the creation of the Deep Web include the forms of operation of the most popular search engines in the world, the lack of digital-information skills of network users and the fact that data providers utilise commercial and restrictive access (Cisek). It is highly important to understand the differences between the Dark Web and the Deep Web. Although the size of the Deep Web is immeasurable, in 2001 it was estimated to be approximately 400 to 500 times larger than Surface Web, namely the internet that is publicly accessible and used daily. On the other hand, the Dark Web incorporates a few thousand encrypted sites constituting 0.01% of the Deep Web.

The Silk Road and its descendants are examples of Dark Net sites. The Silk Road is utilised for buying and selling illegal drugs. However, there are also different applications of the Dark Web. Individuals operating in closed, totalitarian societies may use the Dark Internet to communicate with the outside world. Generally speaking, the Dark Internet mostly serves widely interpreted terrorism.

The list of crimes committed on the Dark Web is extensive. They are enumerated and discussed in detail by Shubhdeep Kaur and Sukhchandan Randhawa from the Thapar University in their work: *Dark Web: A Web of Crimes*. They presented a detailed list of the twelve main types of crime. These include illegal drug trade, human trafficking, the leaking of sensitive information, child pornography, proxying (a form of fraud, scam), the illegal sale of stolen debit and ATM cards, fraud in the domain of Bitcoin (a currency used by network users, also including cybercriminals), illegal weapon trade, "onion cloning" (the redirecting of a user to a false link to convince the user that the site is original; it is related to the stealing of money), contract killings, red rooms (paid, live streams of murders, rapes, tortures, child pornography, etc.) (Kaur, Randhawa, 2020).

Mobile and satellite phones (communication, detonation, etc.), television (mainly used as a form of communication and intimidation – demonstrative decapitations, etc.) and other already-mentioned modern inventions may also serve cyberterrorism. Sometimes, the facilitation of terrorist attacks results from indiscretion and insufficient knowledge of people using a specific technology. Suffice to mention the case from 2018, when the American CIA base in Mogadishu and the Russian air force base in Syria, both secret military facilities, were located based on a map made available through the Strava sports application.

In recent years criminals have started to successfully utilise social media. Even the term *Twitter terrorism* (BBC News) appeared. It is assumed that the Islamic State owns over 50 thousand accounts on Twitter, utilised mostly for communication. Steganography (the communication science that teaches people how to communicate in order to protect

communication against detection) is also commonly utilised. With the use of it, a hidden message is concealed within different content that does not look like a hidden message. Photographs, millions of which may be found on the network, are often utilised for this purpose.

4 Organisations researching the increasing (cyber)terrorism

There are many various organisations researching terrorism and the impact of modern technologies on terrorism all over the world. The studies are conducted mainly to understand how new technologies may be protected against abuse. Only a few of them shall be enumerated here: in Israel – the International Institute for Counter-Terrorism, in the United States – the Office of the Coordinator for Counterterrorism at the U.S. Department of State and START – the Study of Terrorism and Responses to Terrorism – the national consortium of the U.S. Department of State and the University of Maryland. The SAFETY Act (the Support Anti-Terrorism by Fostering Effective Technologies Act) (Cellucci, Davidson, 2011) is also important – the programme adopted in 2002 by the American Congress in response to the attacks of 11 September 2001. In Asia, SATP (South Asia Terrorism Portal) – an organisation researching terrorism and focusing, in particular, on South Asia, has been operating for years.

In addition, more and more research centres dealing with cyberterrorism are being established in European states. ITSTIME – the Italian Team for Security, Terroristic Issues & Managing Emergencies of the Catholic University of the Sacred Heart in Milan – is one of the most interesting. The team, coordinated by Prof. Marco Lombardi, is composed of experts in various fields and competencies. ITSTIME deals with new challenges in the new domain of hybrid war from a theoretical and empirical perspective, focusing mainly on security interpreted as a condition resulting from the establishment and maintenance of protective means capable of promoting the well-being of citizens and the democratic vitality of institutions and terrorism as a long-term risk which needs to be combated by means of well-designed preventive measures and crisis management to develop practices useful for citizens and institutions (ITSTIME).

KCL Cybersecurity Centre operates in London. It is an academic excellence centre operating in the field of research on cybersecurity EPSRC-NCSC (ACE-CSR). It gathers scientists from King's College London dealing with the socio-technical aspects of cybersecurity, including scientists from the Department of Informatics, War Studies, Defence Studies, Digital Humanities and the Policy Institute. Many scientists working over the three main research themes and their interrelations, namely: AI Cyber Security, Formal Cyber Security and Strategic Cyber Security, collaborate with the Centre. The purpose of the Centre is to deliver research to inform about and implement innovations (KCL).

The Cyber Security Academy based in Hague focuses on the development of professional education in the broad sense of cybersecurity in collaboration with LDE universities and

the Hague University of Applied Science. CSA is an initiative of Leiden University, Delft Technical University and the University of Applied Sciences in Hague. The Center for Law and Digital Technologies (eLaw) offers post-gradual studies to professionals working on the organisation of (cyber)security in the private and public sectors (CSA). The Centre examines the social, legal and normative impacts of emerging digital technologies. In the research and education that is conducted, the Centre focuses mainly on digital technologies and their interrelations with basic law and governance.

INIS (The Institute for National and International Security) also plays an important role in the research on cyberterrorism in Europe. INIS is a Scientific Academic Society (recognised by the government of Serbia) promoting security sciences and publishing the "Security Science Journal". And at the same time, it was the first institute in the world that started the analyses of security as a science. INIS gathers academic staff, researchers and scholars to share information and expertise through research papers, situation reports and academic publications for worldwide distribution. It is worth mentioning that INIS administers the largest public domain research database on terrorism and organised crime. The TOC-search (the Terrorist Organised Criminal Search Database) is a dynamic database offering comprehensive information on global terrorist networks and helping researchers, analysts, students and others to prevent terrorism. The INIS mission is to organise and conduct academic and scientific-research activities in the field of national and international security either individually or in collaboration with other, higher education and scientific-research institutions, state bodies, public institutions, enterprises, and civil society organisations.

A young but rapidly developing Polish think-tank is also worth mentioning – the Academic Centre for Cybersecurity Policy (ACCP), operating at the War Studies University in Warsaw whose main goals include, in particular, the preparation of analytical papers (analyses and expert opinions), reports, recommendations and thesis-information materials in the domain of cybersecurity with particular consideration of legal aspects, for the purposes of the Ministry of National Defence, including managerial staff and other entities dealing with cybersecurity in the Republic of Poland. The Information Security Lab is a part of the Centre conducting, among other things, research on cyber-surveillance, cybercrime, cyberterrorism and cyberwar. The Centre also publishes an academic journal titled "The Cybersecurity and Law Journal".

5 Summary

(Cyber)terrorism utilising network technologies is still growing while, at the same time, more and more centres combating it are being established. Information and communication technologies influence every human being and each domain of life. By simplifying communication, the technologies have made our lives easier. However, some new, previously unknown threats have also emerged. The last twenty years have brought about huge transformations in the world of technology. The most vivid example of this is the evolution of the mobile phone that, at the beginning of the nineties, was considered a

luxury, and today, people use PDA equipment as a tool facilitating communication in nearly each and every process of communication. The transformation, referred to by some authors as "technology development" was an incentive for an economic race among countries and organisations. However, it has also become an incentive for a race among the world of crime and those who fight it. So, are network technologies socially useful? The answer is not as easy as it seems. While, on the one hand, the answer is definitely affirmative, on the other, network technologies are a source of serious risks connected with the fact that they are utilised by unauthorised people in an improper way. Nevertheless, the dilemma has been true in the case of each type of technology since its onset. The social rating of technologies is not easy but it is needed because technological development, accompanied by social development, does not necessarily or always have to serve the greater good of society.

References:

Bjørgo, T. (2005) *Root causes of terrorism: myths, reality and ways forward* (London, New York: Routledge).

Castells, M. (2007) *Społeczeństwo sieci* (Warszawa: PWN).

Cairncross, F. (1997) *The Death of Distance: How the Communications Revolution Will Change Our Lives* (Boston, MA: Harvard Business School Press).

Cellucci, T.A. & Davidson, B. (2011) *SAFETY Act: Adding Value through Strategic Deployment* (U.S. Department of Homeland Security).

Denning, D. (2000) *"Cyberterrorism", Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services* (US House of Representatives).

Gamm, G.U., Sester, S. & Reindl, L. (2013) SmartGate - Connecting wireless sensor nodes to the Internet, *Journal of Sensors and Sensor Systems*, 2(1), pp. 45-50.

Koechler, H. (2002) *The United Nations, the international rule of law and terrorism*, Fourteenth Centennial Lecture, Supreme Court of the Philippines & Philippine Judicial Academy, available at: http://hanskoechler.com/koechler-IRLUN-Berlin-Jan05.htm (August 30, 2022).

Kosikowski, C. (2016) Nowe Prawo rynku finansowego Unii Europejskiej, In: Jurkowska-Zeidler, A. & Olszak, M. (eds.) *Prawo Rynku Finansowego. Doktryna, instytucje, praktyka* (Warszawa: Wolters Kluwer), pp. 27-38.

Lyon, D. (2007) *Surveillance Studies: An Overview* (Cambridge: Polity Press).

Marszałek, M. (2009) *Sojusznicza operacja "Allied Force": przebieg - ocena – wnioski* (Toruń: Wydawnictwo Adam Marszałek).

Minsky, M., Kurzweil, R. & Mann, S. (2013) *The Society of Intelligent Veillance*, Proceedings of the IEEE ISTAS 2013 (Toronto, Ontario, Canada), pp. 13-17.

National Research Council (1991) *Computers at Risk* (Washington, DC: National Academy Press).

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M. & Gagnon, G. (1999) *Cyberterror. Prospects and Implications*, White paper, available at: https://calhoun.nps.edu/bitstream/handle/10945/27344/Cyberterror%20Prospects%20and%20Implications.pdf?sequence=1&isAllowed=y (August 30, 2022).

Nowacki, G. (2002) *Rozpoznanie satelitarne USA i Federacji Rosyjskiej* (Warszawa: Akademia Obrony Narodowej).

FRA (2010) *Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu: przewodnik* (Luksemburg: Urząd Publikacji Unii Europejskiej).

Record, J. (2003) *Bounding the global war on Terrorism* (Strategic Studies Institute).
Sandler, T. & Enders W. (2011) *The Political Economy of Terrorism* (Cambridge: Cambridge University Press).
Wasiuta, O. (2019) Dark Web, In: Wasiuta, O. & Klepka, R. (eds.) *Vademecum bezpieczeństwa informacyjnego* (Kraków: Instytut Nauk o Bezpieczeństwie, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej), pp. 251-256.

.

The Role of Cybersecurity in the Public Sphere - The European Dimension. Financial Institutions

PAWEŁ PELC

Abstract The subject-matter of the analysis includes the state of the EU legal framework and the proposed amendments in the sphere of the cybersecurity of financial institutions operating in European Union Member States, interests protected by law, and the rationale behind regulatory provisions proposed or adopted by EU legislators, notwithstanding their legal form (strategic documents, directives or regulations).

Keywords: • European Union • cybersecurity • financial institutions • financial market • digital resilience

CORRESPONDENCE ADDRESS: Paweł Pelc, Attorney at law, Ph.D. Student, War Studies University in Warsaw, Academic Centre for Cybersecurity Policy, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

https://doi.org/10.4335/2022.2.4 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

This analysis discusses the current and planned EU legal regulations governing the cybersecurity of financial institutions, including the assessment of the premises behind selected regulatory solutions, the role of provisions in respect of the cybersecurity of financial institutions in the context of the objectives and directions of regulations concerning financial institutions in the European Union, adopted in the aftermath of the 2007-2008 financial crisis, including the protection of the public sphere against the consequences of threats which affect financial institutions.

Given the specific nature of cyber threats which are usually of a cross-border nature and are not limited to individual jurisdictions, which results in the internationalisation of both attacks and responses, as well as of their impact (both direct and indirect impact through the "contagion effect"), the European Union is becoming increasingly active in enacting legal regulations in this respect. (The current European Union's initiatives in the sphere of cybersecurity have been discussed by Naydenov and Theacharidou, 2021).

In December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented The EU's Cybersecurity Strategy for the Digital Decade (European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2020). In the document, it has been found that cybersecurity constitutes an integral part of security, and is essential for building a resilient, green and digital Europe. The authors also pointed to the increased vulnerability of cyber-attacks in relation to switching to remote work due to the COVID-19 pandemic. The risk of targeting critical infrastructure was also noted. The strategy clearly points to the scale of cyber-attacks on the finance sector.

In June 2021, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published their Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade (European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2021). The authors pointed to the key significance of the fastest possible adoption of proposed legal regulations, including the Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/1148, COM (2020) 823, the Proposal for a Directive on the resilience of critical entities, COM (2020) 829, Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014, COM (2020) 595, and the Proposal for a directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, COM(2020) 596.

The first of the above documents is the European Commission's Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/1148. It is to replace Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information

systems across the Union (NIS Directive) (OJ EU L 194 of 19.7.2016, p. 1) which is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the Union (Krueger, Brauchle, 2021: 16-17). According to the Recitals of this Directive: "Operational risk is a crucial part of prudential regulation and supervision in the sectors of banking and financial market infrastructure. It covers all operations including the security, integrity and resilience of network and information systems. The requirements in respect of those systems, which often exceed the requirements provided for under this Directive, are set out in a number of Union legal acts, including: rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and rules on prudential requirements for credit institutions and investment firms, which include requirements concerning operational risk; rules on markets in financial instruments, which include requirements concerning risk assessment for investment firms and for regulated markets; rules on OTC derivatives, central counterparties and trade repositories, which include requirements concerning operational risk for central counterparties and trade repositories; and rules on improving securities settlement in the Union and on central securities depositories, which include requirements concerning operational risk. Furthermore, requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. Member States should consider those rules and requirements in their application of lex specialis" (OJ EU, L 194 of 19.7.2016, p. 1, Recital 13). The Directive includes, i.a., credit institutions, trading systems and central counterparties in the group of critical sectors it refers to.

In line with the Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/114, the draft Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014, COM (2020) 595, subject to concurrent pending legislative procedure, will be considered to be a sector-specific Union legal act with regard to the financial sector entities, and the provisions of the proposed regulation relating to information and communications technology (ICT) risk management measures, the management of ICT-related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third-party risk should apply instead of those set up under the proposed Directive. Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.

The second draft act mentioned in the Report on implementation of the EU's Cybersecurity strategy is the Proposal for a Directive on the resilience of critical entities. The proposal aims to enhance the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities by increasing the resilience of critical entities providing such services. The European Commission has found that, since the EU financial services acquis establishes comprehensive

requirements on financial entities to manage all risks they face, including operational risks and ensuring business continuity, those entities should be treated as equivalent to critical entities, and the proposed Directive would not involve any additional obligations on the part of financial entities (European Commission, 2020b, Recital 15). The proposal indicates the following EU legal regulations addressed to the financial sector taking into account the issues of cybersecurity: Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ EU L 201, 27.7.2012, p. 1), Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ EU L 173, 12.6.2014, p. 349), Regulation (EU) No. 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No. 648/2012 (OJ EU L 173, 12.6.2014, p. 84), Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012 (OJ EU L 176, 27.6.2013, p. 1), and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ EU L 176, 27.6.2013, p. 338).

As regards operational risk management in the sphere of the cybersecurity of a number of financial institutions, particular importance can be assigned to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC (OJ EU 337, 23.12.2015, p. 35) ("PSD 2"). It stipulates that payment service providers are responsible for security measures which need to be proportionate to the security risks concerned. They should also establish a framework to mitigate risks and maintain effective incident management procedures. A vital part of this law is the establishment of a regular reporting mechanism, in order to ensure that payment service providers provide the competent authorities, on a regular basis, with an updated assessment of their security risks and the measures that they have taken in response to those risks. The obligation to report major security incidents without undue delay to the competent authorities was also introduced (OJ EU 337, 23.12.2015, p. 35, Recital 91). It was also found that payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud, while a solid growth of Internet payments and mobile payments should be accompanied by a generalised enhancement of security measures which should be compatible with the level of risk involved in the payment service (OJ EU 337, 23.12.2015, p. 35, Recitals 95 and 96). This was the first EU law addressed to the financial sector which expressly set out cybersecurity requirements (Krueger, Brauchle, 2021: 14).

The third draft act indicated in the Report on implementation of the EU's Cybersecurity Strategy is the Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014 ("DORA"). The said proposal is part of the digital finance package, which is a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it. The digital finance package includes a new Strategy on digital finance for the EU financial sector (European Commission, 2020). The European Commission is of the opinion that it is necessary to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities, with a view to deepening the digital risk management dimension of the Single Rulebook. The starting point for the above decisions was the acknowledgement of the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, which may result in a situation where localised cyber incidents could quickly spread from any of the Union financial entities to the entire financial system, unhindered by geographical boundaries (European Commission, 2020d, Recital 3). According to the European Commission, it is crucial to maintain a strong relationship between the financial sector and the Union horizontal cybersecurity framework, as it would ensure consistency with the cybersecurity strategies already adopted by Member States, and allow financial supervisors to be made aware of the cyber incidents affecting other sectors covered by the NIS Directive (European Commission, 2020d, Recital 16). The European Commission also pointed out that the significant consequences of cyber-attacks are amplified when occurring in the financial sector, an area much more at risk of being the target of malicious propagators pursuing financial gains directly at the source (European Commission, 2020d, Recital 42). In line with the proposed regulation, "digital operational resilience" means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly (through the use of services of ICT third-party providers), the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provisions of financial services and their quality ((European Commission, 2020d, Article 3(1)), while "cyber-attack" means a malicious ICT-related incident by means of an attempt to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset perpetrated by any threat actor (European Commission, 2020d, Article 3(9)). The proposed DORA will have a significant impact on cybersecurity measures taken by numerous financial institutions covered by the scope of this regulation, also through the introduction of a requirement to conduct penetration tests affecting a lot of those entities.

The fourth draft act mentioned in the Report on implementation of the EU's cybersecurity strategy is the Proposal for a directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36,

2014/65/EU, (EU) 2015/2366 and EU/2016/2341. It is part of a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it. It complements the DORA proposal and the legal regulations on markets in crypto assets currently being developed. It aligns the directives subject to amendment of the provisions included in the DORA proposal. It has been found that the need to ensure the operational resilience of digital operations in the financial sector against ICT risks has become particularly pressing because of the growth in the market of breakthrough technologies, including those related to crypto assets (distributed ledger or similar technology).

In the Digital Finance Strategy for the EU, the European Commission stated that "the future of finance is digital." Therefore, one of the priorities described in the Strategy is to address new challenges and risks associated with digital transformation. The European Commission believes that technology companies are likely to become an integral part of the financial ecosystem, and, as a consequence, the risks are expected to increase, affecting not only customers of financial institutions, but also broader financial stability issues and competition in financial services markets. Therefore, the prudential supervisory perimeter should capture risks arising from platforms' and technology firms' financial services provisions and from techno-financial conglomerates and groups. According to the European Commission, the EU cannot afford to have the operational resilience and security of its digital financial infrastructure and services called into question. There is also a need to minimise the risk of client funds being stolen or their data being compromised. The objective of the European Commission's activities in this respect is to protect end users of digital finance services, to ensure financial stability, to protect the integrity of the EU finance sector and to provide fair conditions for operation.

The requirement to implement appropriate technical and organisational measures in the scope of personal data processing has been imposed on financial institutions under Articles 32-34 of the GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/ 46/EC (General Data Protection Regulation), (OJ EU L 119, 4.5.2016, p 1).

The aforementioned legal regulations are addressed to private organisations running regulated business activities subject to oversight, either at the EU level or in individual Member States. They result from the recognition of their special functions and their impact going beyond the operations of individual institutions. It is a consequence of recognising the special role of the financial market and the need to protect the customers of finance institutions and to ensure the uninterrupted functioning of institutions operating in this market, and the performance of their tasks.

In the opinion of the European Commission, both the organisation of the financial market and the regulation governing its operations need to ensure security of the participants in

this market. Some of the essential components of the market include the provision of access to that market to licensed entities, the oversight of their operations, and prudential requirements (Kosikowski, 2016: 27-38). Significant changes in this respect were introduced in the European Union after the experience of the financial crisis of 2007-2008 (Kosikowski, 2016: 31-38; Monkiewicz, 2016: 59-73; Kluczewska-Rupka, 2015: 91-105). As a consequence of the growing number of cybersecurity threats, legal regulations concerning cybersecurity and critical infrastructure, including sector-specific regulations in this respect referring to financial institutions or their individual categories, were introduced and further expanded. Provisions in the sphere of cybersecurity were included in Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012 (OJ EU L. 176, 27.6.2013, p. 1), and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, as well as PSD 2 and Regulation of the European Central Bank (EU) No. 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ EU L217, 23.7.2014, p. 16), whereas no such explicit cybersecurity rules were provided in Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ EU L335, 17.12.2009, p. 1), Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU, and Regulation (EU) No. 236/2012 (OJ EU L 257, 28.8.2014, p. 1), and Regulation (EC) No. 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies (OJ EU L 302, 17.11.2009, p.1) (Krueger, Brauchle, 2021: 15). The evolution of the financial market, together with its globalisation and cross-border activities, and the growing scale of the interrelations between individual financial institutions, results in an increased risk of volatility in the case of problems of individual financial institutions, expanding across the entire financial market (Nieborak, 2016: 94-112), which might trigger a shift to the so called "real economy". Consequently, the regulations concerning the financial market are aimed to mitigate the risk of impact of the operations of financial institutions in the public sector, including public finance. A good example of such an approach can be found in the solutions included in the Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms, and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations

(EU) No. 1093/2010 and (EU) No. 648/2012, of the European Parliament and of the Council (OJ EU L 173, 12.6.2014, p. 190), in accordance with which recovery and resolution plans should not assume access to extraordinary public financial support or expose taxpayers to the risk of loss (OJ EU L 173, 12.6.2014, p. 190; Recital 31), and a failing institution should be maintained through the use of resolution tools as a going concern with the use, to the extent possible, of private funds (OJ EU L 173, 12.6.2014, p. 190; Recital 46), while an effective resolution regime should minimise the costs of the resolution of a failing institution borne by taxpayers (OJ EU L 173, 12.6.2014, p. 190; Recital 67). Public interest was taken into account in these legal provisions, as a vital element which allows the application of mechanisms set out in relevant EU legal regulations in respect of financial institutions. "(...) Liquidation under normal insolvency proceedings might jeopardise financial stability, interrupt the provision of critical functions, and affect the protection of depositors. In such a case, it is highly likely that there would be a public interest in placing the institution under resolution and applying resolution tools rather than resorting to normal insolvency proceedings. The objectives of resolution should, therefore, be to ensure the continuity of critical functions, to avoid adverse effects on financial stability, to protect public funds by minimising reliance on extraordinary public financial support to failing institutions, and to protect covered depositors, investors, client funds and client assets." (OJ EU L 173, 12.6.2014, p. 190; Recital 45). Given the above, it should be stated that EU regulations addressed to financial institutions, as a rule private market entities, are aimed to protect a broadly understood public sphere, in order to avoid threats to public funds, financial stability, and only after that the interests of clients of such institutions, although the legal provisions are also far reaching in this respect. The European Commission proposed the extension of consumer protection provided for in Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, (OJ EU L133, 22.5.2008, p. 66) by putting forward the Proposal for a Directive of the European Parliament and of the Council on consumer credits, COM/2021/347 final, i.a., due to the consequences of digital transformation (European Commission, 2021, Recitals 3 and 4). The assurance of the digital resilience of financial institutions, including measures to prevent the contagion effect, are part of the activities (Krueger, Brauchle, 2021: 25-26). Similarly, as in the case of supervision mechanisms, where supervisory authorities shifted from oversight based on the assurance of supervised institutions' compliance with applicable regulations to risk-based supervision, the regulations currently being proposed by the European Commission envisage the financial institutions' transfer from assuring compliance with regulations in the scope of security to management based on the assessment of risk and threats related to their operations. This is owing, i.a., to the perception of cyber threats and cyber risks as a systemic risk affecting the financial sector (European Systemic Risk Board, 2020: 2-3 and 22-39). The European Systemic Risk Board noted the following possibility for a cyber-attack to develop into a threat to the stability of the financial system: "From a macroprudential perspective, the ESRB considers the main shocks to be the destruction, encryption or alteration of data related to value. Such shocks could cause a cyber incident to develop

into a systemic event, impairing the provision of key economic functions, generating significant financial losses and undermining confidence in the financial system" (European Systemic Risk Board, 2020: 3), while such risk was also pointed out by Callies and Baumgarten (Callies, Baumgarten 2020: 1150-1151). The perception of issues related to the cybersecurity of financial institutions and respective legal regulations as a vital part of the security of the public sphere is all the more important considering that the attribution of attack sources is not always clear-cut and that such attacks may be an element of cyber war (for instance as part of the so-called hybrid war), cyber espionage, or cyber terrorism, for which public or parastatal actors may be responsible. Even if an attack is classified as a mere cyber offence, it cannot be ruled out that such cyber criminals are supported or at least tolerated by public actors. Consequently, the public security element is particularly visible in the way the issues related to the cybersecurity of financial institutions are regulated in the European Union. This is also demonstrated in the legal basis for EU cybersecurity laws which are based on the provisions of the Treaty on the Functioning of the European Union referring to freedom, security and justice, the freedom of services, and the smooth operation of payment systems (Callies, Baumgarten, 2020: 1163-1164).

Given the above, it can be stated that the regulations concerning the cybersecurity of financial institutions take into account the specific nature and directions of EU laws addressed to financial institutions, so as to protect the public sphere against threats emerging in relation to the activities pursued by such entities. Therefore, the introduction of separate sector-specific regulations addressed to financial institutions, which are to replace general cybersecurity regulations, should be considered as reasonable. Thanks to this, these solutions may take into account the specific risks which occur in the course of financial institutions' operations, and the EU legislator's preferences in the sphere of protected public interest in relation to such risks.

References:

Callies, C. & Baumgarten, A. (2020) Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective, *German Law Journal*, 21(6), pp. 1149-1179.

Kosikowski, C. (2016) Nowe Prawo rynku finansowego Unii Europejskiej, In: Jurkowska-Zeidler, A. & Olszak, M. (eds.) *Prawo Rynku Finansowego. Doktryna, instytucje, praktyka* (Warsaw: Wolters Kluwer), pp. 27-38.

Kluczewska-Rupka, A. (2015) Dylematy prawne powołania europejskiej Unii Bankowej, In: Rogowski, W. (ed.) *Polityka i praktyka regulacji rynków finansowych* (Kraków-Warsaw: Oficyna Allerhanda), pp. 91-105.

Krueger, P.S. & Brauchle, J.P. (2021) *The European Union Cybersecurity, and the Financial Sector: A Primer* (Washington DC: Carnegie Endowment for International Peace).

Monkiewicz, J. (2016) Unia Bankowa jako zmiana architektury regulacyjnej i nadzorczej rynku finansowego z perspektywy ekonomicznej, In Jurkowska-Zeidler, A. & Olszak, M. (eds.) *Prawo Rynku Finansowego. Doktryna, instytucje, praktyka* (Warsaw: Wolters Kluwer), pp. 59-73.

Naydenov, R. & Theocharidou, M. (2021) *EU Cybersecurity initiatives in the finance sector* (Athens: European Union Agency for Cybersecurity).

Nieborak, T. (2016) Unia bankowa – w stronę bezpieczeństwa i stabilności rynku finansowego Unii Europejskiej, In: Jurkowska-Zeidler, A. & Olszak, M. (eds.) *Prawo Rynku Finansowego. Doktryna, instytucje, praktyka* (Warsaw: Wolters Kluwer), pp. 94-112.

Strategic and Political Responsibility in the Domain of Cybersecurity - Problems and Challenges

ANNA MAKUCH

Abstract Strategic and political responsibility which, based on the knowledge of the specific character of cyberspace, allows for a conscious and meaningful use of internet resources, is considered a key factor in eliminating threats to the digital data exchange environment. As contemporary infosphere promotes intuitive patterns of navigating and using open resources, it seems imperative to promote the principles of responsibility by popularising cyber hygiene and information ecology, which contribute to both the safety of users and system security within the national dimension of cyberspace.

Keywords: • responsibility • political system • security in cyberspace • information security

CORRESPONDENCE ADDRESS: Anna Makuch, Ph.D., Researcher-academic, University of Economics and Human Sciences in Warsaw, Faculty of Political Science, Department of Social Sciences, Ul. Okopowa 59, 01-043 Warsaw, Poland, e-mail: a.makuch@vizja.pl, ORCID: 0000-0002-5222-4407.

https://doi.org/10.4335/2022.2.5 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

Not all soldiers are warriors and not all warriors are soldiers.
J.J. Patrick, 2018, the Art of Hybrid War.

1 Introduction

Attention is mainly focused on identifying the key challenges related to the strategic and political responsibility in the domain of cybersecurity (Pawłowski, Zdrodowski, Kuliczkowski, 2020: 38).

Such formulation of the topic suggests, firstly, that the concept of responsibility under analysis is important enough to make an effort to sort out the research issues; secondly, that attention will be focused on the specific character of responsibility in the digital space, taking into account both the architecture and infrastructure of this domain (Chałubińska-Jentkiewicz, 2019); and thirdly, that the dimension of responsibility has been undergoing transformation in the age of digitisation – just as digitisation has influenced the fundamental transformation of social, political, economic and cultural arrangements. This influence has manifested itself in a trend, visible for more than two decades, of shifting activities into digital space where information has become a more important commodity than tangible products (Castells, 2013: 25, Sartori, 2007).

The network of digital connections, being rhizomatic or nomadic according to Deleuze and Guattari (Deluze, Guattari, 1980), constitutes a "central nervous system" of the globalised information environment, in relation to which traditional forms of communication (paper press, radio news, television) appear to be secondary and retarded. The revolutionary dimension of this new intangible domain has not been limited to the function of storage in the created space, but has additionally resulted in a series of transformations in each area of human activity – in the field of media systems with new forms, i.e., hybridity and live participation in programmes, and in the field of social communication, e.g., social media.

The strategic and political perspective implies that the analysis of responsibility, in terms of the geography of digital space, exhibits two dimensions. The first dimension concerns the national system (Pawłowski, Zdrodowski, Kuliczkowski, 2020: 212) while the second one pertains to the level of international relations, encompassing interactions, decisions, and their social and political consequences affecting their participants. In the international dimension, the outcome of activities carried out by entities corresponds to the real effect induced by favourable decisions that match actual interests. At present, due to significant transformations of the public domain, the national dimension continues to gain importance. The outreach and use of cyberspace by individual users forms one of the factors influencing transformation in this domain – the launching of digital communication platforms has triggered a phenomenon of public diplomacy involving content resonance from each participant in the content exchange process. Modern techniques of information management enable individual users to build a platform of

influence covering a national or global system. It is not without essence that the objectives and motives of actions are authentic, as they are revealed in the course of activities and may expose manipulative or socially-harmful intentions.

Referring to the Congress of Vienna, during which a new balance of power was created through negotiations between a small circle of the political elite, the difference stems from the incomparably greater influence of individuals in the processes of interest aggregation, shaping public opinions through the exchange of messages, or influencing public views, especially if an organised destabilising activity is identified (Volkoff, 1991: 8). Therefore, as regards the national system security, individual users' activities should now be the focus of attention of dedicated services, given their potentially wide ranging influence.

The combination of the political aspect with the strategic aspect seemingly only simplifies the taxonomy – on the one hand, it prescribes certain activities within the national system and, on the other hand, through the very structure of the internet, it triggers the need to take into account the global system, with which it forms the nomadic and deterritorialised network referred to by Deleuze and Guattari. As part of the national system, the constitutive features and objectives of the state, implemented through the structures and components of the political system, are considered a priority. These primarily include the category of the security of citizens forming a community, and security of the political system as a tool for implementing this generally formulated objective (from a philosophical point of view, security is composed of three levels: survival, elimination of threats, and development) (Świniarski, 1999: 13). While the subjective scope encompasses all citizens of a given state, the objective one has grown considerably, for instance, in comparison to the 19th century, giving rise to continually-developing sectoral areas (energy security, maritime security, ecological security, water resources security, to name a few).

Digital deterritorialisation in the 20th century was accompanied by the decreasing importance of physical state borders as a consequence of the ongoing globalisation processes which involved internationalisation, institutionalisation and integration of transnational processes. While technological progress made it possible, as the poet prophetically put it, „[t]o see a world in a grain of sand and a heaven in a wild flower / hold infinity in the palm of your hand, and eternity in an hour", the nature of the technological tool exposed some threats in the areas of personal, group, national and global security. At the same time, it became a catalyst for revealing numerous problems related to participating in cyberspace (Open Source Intelligence Investigation, 2016), which has become a field of competition between economic, political and other actors (Dela, 2020: 15). Problems arising from network use also relate to the violation of system security structures, financial and sexual crime (Internet Organised Crime Threat Assessment IOCTA, 2020), the right to privacy, and cyberterrorism (Soler: 2015, 497-499).

2 Responsibility – its philosophical, political and strategic dimensions – taxonomy

Since the beginning of European philosophical reflection, the category of political responsibility has created numerous problems in terms of meaning, definition and legislation. The dilemmas present over the centuries have not been exhaustively explained or resolved, while the circumstances changed by the digitisation of social life have posed new challenges.

Heywood divided the categories of responsibility into three main sections: 1) responsibility for someone or something (for oneself or society); 2) responsibility to someone, which is viewed as *stricte* political, as it refers to the supervisory body (Robertson, 2009: 281); and 3) responsibility as an ethical action regardless of certain influence or circumstances (e.g., the potential decline in popularity or support) (Heywood, 2008: 127). L. Strauss, in turn, noted that nowadays we attach a different meaning to the concept of responsibility – it implies, as a matter of fact, breaking with the tradition of defining and understanding responsibility as synonymous with "being just, right, virtuous" (Strauss, 1998: 258). Following the line of thinking adopted by L. Strauss, it can be assumed that the political dimension now prevails over the ethical dimension, which forms the main axis for contemporary arguments (Tinder, 2003: 133.158).

In the 20th century, reflections on responsibility were the main focus of attention for many fields and disciplines due to the experience of totalitarianism and the world wars. The exchange of ideas influenced the development of human rights and significantly diversified philosophical reflections, with the German-Austrian and French centres paving the way for leading trends (Filek, 2004). The themes taken up from various points contributed to the evolution of the 20th-century narration on responsibility towards a community-based or social perspective of responsibility, indicating its ethical dimension, escaping detailed characterisation. This was also the direction followed by H. Jonas who criticised the concept of "empty formal responsibility" (Filek, 2004: 208).

As part of the philosophical discourse on responsibility, the dimension of freedom conditioning the emergence of responsibility is emphasised. "If we deny the existence of freedom, we deny the existence of responsibility" (Nowicka-Kozioł, 1993: 25, Krąpiec, 1991: 272). In other words, freedom is required for responsibility to arise, and a sense of responsibility is fostered by freedom. This was an axiom which did not raise substantial doubt in the scientific literature of the 20th century, however, a few reservations could be found in this area. One of these was formulated by Hallowell, pointing to the 20th-century tendency of societies to escape responsibility. He wrote: "It was the previous rejection of the verdicts of conscience that enabled Hitler to rise to power" (Hallowell, 1993: 48). Hallowell's assessment did not take into account the difficult economic circumstances of

the post-war crisis, which proves that responsibility for social life was of fundamental importance for this researcher.

20th-century reflection touches upon the problem of the unlawful deprivation of the liberty of individuals in totalitarian systems as a result of the self-deprivation of responsibility, posing threats to the freedom of life and property. In the case commented on by Hallowell, we are dealing with the incorrect self-identification of the situation by citizens, which led to the collapse of the rule of law and the introduction of a state of emergency (Ryszka, 1974). It should be, nonetheless, emphasised that the consequence of the transfer of power in Western or Central European systems reflected an attempt made by citizens to diagnose the socio-political situation on the basis of the available electoral offer. Individual decisions affected society at large, which proved revolutionary as regards its consequences (M. Nowicka-Kozioł, 1993: 8). The transfer of responsibility was effected: 1) by virtue of the incorrect materialisation of the common good in the form of a charismatic leader, or 2) solely with the intention of giving up responsibility, as described by Hallowell, which is, in a way, automatically linked to giving up freedom.

The prevailing contemporary paradigm of the democratic rule of law rests on the foundation of what is considered a set of universal principles of human rights (Robertson: 2009, 343; Universal Declaration of Human Rights of 10 December 1948). The list of these rights has been greatly expanded over the centuries, and today one can even speak of fifth-generation human rights (Zubik, 2008: 6). In western civilisation, the rights to life, property, freedom of conscience, religion, opinion and assembly constitute an established set of principles and values. From a systemic point of view, in western culture the problem of unlawful deprivation of subjective freedoms, based on inalienable human rights intrinsically connected with human dignity, does not exist. One of the principles of a democratic system, namely mutual control based on responsibility, serves both the state and its citizens, forming the axis of a modern democratic governance pattern. It also supports the transparency of the human rights protection process.

The structure, character and ways of using cyberspace influence the reactions of political systems toward information security threats, including threats to data and content manipulation. The necessary element of self-identification of the situation from the angle of its possible consequences, which requires self-reflection, is unrealistic in an era of overproduced information, fast transmissions and huge amounts of information exceeding the capacity of human perception. A contemporary culture of connectivity, based on externalised data and portable databases (Assmann, 2019: 27), not only discourages self-reflection but also promotes a model of non-linear and nomadic culture, presenting the ballast of in-depth analysis as a burden of encyclopaedic knowledge that has become useless in an age of "social competence" and portable digital resources. In turn, being cut off from the deposit of memory and knowledge organised according to the principles of scientific cognition makes it impossible to analyse the problems of network use in an appropriate comparative context. Therefore, the contemporary environment of digital

information is actually becoming conducive to disinformation and manipulation (manipulation is "a way of exerting influence on other people or groups in order to induce changes in their behaviour and conduct. By definition, this mechanism is supposed to influence the subconscious mind of a manipulated person or group in a covert manner") (Harwas-Napierała, 2005: 287) of all activities to gain informational advantage corresponding to the ontological level of war. This non-military dimension is consistent with tactical recommendations by Sun Zi, emphasising the benefits of defeating an enemy at the lowest possible cost and even before a clash of arms. In cyberspace, non-military methods are used, based on psychological techniques of exerting influence, the effectiveness of which lies not in putting forward arguments for the recipient to evaluate them, but in a much more sophisticated method of shaping preferences according to the sender's intention. A separation from verification sources or a belief that they are unnecessary leads to a weakened resistance to psycho-manipulation and thus also to increased other-directedness, the latter being destructive for the sovereignty of the national system as it disturbs the communication balance within the system.

Manipulation in an environment preventing the verification and unbiased assessment of delivered content presents serious ground for making attempts to identify a direction to counteract both information and systemic threats in cyberspace. A component anticipating threats – based on the principles of effective operation (Sennet, 2010), or belonging to the indirect operation strategy (Liddell-Hart, 1959: 13), i.e., promoting a culture of the responsible use of cyberspace, could be considered crucial. Ingarden's "source of decisions" – the person – relies on the understanding of a given situation and a determination to act – in opposition to intuitive action (Ingarden, 1987: 77), while the contemporary navigation of cyberspace is based on an intuitive model of action, cutting to a minimum the need to perform a situation analysis. The speed, dynamics and overproduction of data do not favour moments of self-reflection or verification, and according to philosophical schools of thought, these are the *sine qua non* conditions of responsibility which is indispensable for ensuring strategic and political security and without which it is impossible to achieve.

The challenge of formulating ways to support political and strategic responsibility, as a factor contributing to network security at individual and national levels, is becoming a pertinent matter.

3 The notion of responsibility vs. cybersecurity

The internet, as a meta-medium brought into common use, has blurred the boundaries between the private and public spheres of communication and data acquisition – by having a mobile device with access to a network at our disposal, we automatically become participants of the global exchange of data and messages, whether passive or active, thus influencing the information environment, the centre of which is cyberspace, where the object of attention is information. A user is able to combine his/her professional duties

and private interests in one place and with one medium (i.e., to book a concert ticket while at work, to draw up a report during breaks from taking care of the children, etc.). Over the years, the dynamics of sharing content via online portals or social networks has been increasing. The high rate of network subjectification and the perception of one's own participation as negligible and strictly private influences self-positioning in the digital space in terms of a sense of security and anonymity (Baran, Cichocka, Maranowski. and Pander, 2016). This illusory sense underpins the success of cybercrime which exploits the unawareness of cyberthreats among individual users and employees who disseminate personal or company data in cyberspace. The methods and techniques employed by cybercriminals against individual users are more often simple, which confirms the fact that elementary cybersecurity mechanisms for network users are far from widespread (Kronenberg Foundation, 2020).

The nature and essence of the internet, as a rhizomatic networked matrix of connections, contributes to a reduced sense of responsibility with respect to the vastness of content and apparent user anonymity. Relatively cheap access to data resources makes the internet a tool for facilitating work, learning and entertainment. In the field of data exchange infrastructure (e.g., e-government, remote work), the internet performs the function of somehow liberalising professional life although this type of a resource is also the subject of cyber warfare within OSINT activities. As regards social life, commerce and politics, the internet offers not only a means of free participation and favourable solutions for data administration, services, commerce and entertainment, but it also opens up multiple opportunities for the manipulation of information, preferences and attitudes by means of Big Data and by implementing AI algorithms.

In view of the above considerations, it appears justified to take measures aimed at strengthening political and strategic responsibility as a factor that exerts a positive impact on the security of network use and the systemic security of the state. The notion of strategy, as defined by Liddell-Hart (Liddell-Hart, 1959: 13) stands for "general command" and "day-to-day management of military forces", but the decision to use them, as Liddell was right to note, is dependent on politicians and the custodians of national system security. Given the competitive nature of cyberspace, disseminating the principles of security contradicts the interests of those entities which hope for the citizens to remain credulous and to ignorantly share valuable personal data (Chałubińska-Jentkiewicz, Nowikowska, 2021). It is required: 1) to popularise the perception of the internet as being by nature a disinformation tool; 2) to promote actions in the statutory area (the National Cyber Security System Act of 5 July 2018); 3) to take tactical and operational action in terms of building an information culture based on the principles of cyber hygiene and information ecology (Taraszkiewicz, 2014).

Cyberspace is a reflection of users' interests and needs, rather than of reality (Dela, 2020: 20). The mechanisms that foster a responsibility culture in which decisions and evaluations reflect judgements, rational calculations, the mapping of possible

consequences on a timeline, and the choice of a favourable direction, require a broad promotion of knowledge about the contemporary information environment and the possible consequences of imprudent participation.

4 Conclusions

The reactivation of the culture of strategic and political responsibility will produce a tangible effect through disseminating knowledge of the nature of the internet and the threats it poses, among which the following issues are important: 1) knowledge of the functioning and specificity of the digital infosphere environment – positioning the user as an object of attention of commercial and political actors in order for them to be included in Big Data analysis systems and acquired for particular purposes (commercial and political persuasion); 2) knowledge of the viability of displayed content and its importance in the context of OSINT activities or the cybercrime sector (e.g., phishing); sharing knowledge about one's private life (a new car, a trip) constitutes valuable information which enables building a user's profile for personalised commercial offers, but it also provides criminals with information regarding access to one's real estate; 3) awareness regarding the impact of the overproduction of stimuli and information violence, which both affect the functioning of the human brain (a loss of abstract thinking skills or the reduced ability to process information impulses), decreased ability to concentrate, irritability, information addiction, desensitization, infotainment-related threats (Babik, 2014: 7-19); 4) disseminating knowledge of systemic security tools (two-step security codes, firewalls); 5) attaching adequate importance to regulations and rules which accompany granting consent to use resources, and which point out the potential danger of granting consent to access one's personal data; 6) emphasising how important personal data are these days and the fact that they constitute knowledge capital for commercial entities, media houses, analysts of political life, etc.

The popularisation of knowledge about the digital infosphere has the potential to strengthen the defence mechanisms in society and the level of resistance to threats, and thus to foster the tendencies of increasing responsibility for the content shared and received in the political and strategic dimension, which concludes the arguments presented in this paper.

References:

Assmann, J. (2019) *Pamięć kulturowa. Pismo, zapamiętywanie i polityczna tożsamość w cywilizacjach starożytnych* (Warszawa: Wydawnictwa Uniwersytetu Warszawskiego).

Babik, W. (2014) O konsumpcji informacji w e-społeczeństwie z punktu widzenia ekologii informacji, In: Taraszkiewicz, B. (ed.) *Ekologia informacji w e-społeczeństwie* (Słupsk: Stowarzyszenie Bibliotekarzy Polskich - Zarząd Oddziału Słupskiego, Biblioteka Uczelniana Akademii Pomorskiej w Słupsku, Pedagogiczna Biblioteka Wojewódzka w Słupsku), pp. 7-25, available at:

https://depot.ceon.pl/bitstream/handle/123456789/17699/Ekologia%20informacji%20-%20Taraszkiewicz.pdf?sequence=1&isAllowed=y (September 20, 2021).

Baran, M., Cichocka, E., Maranowski, P. & Pander, W. (2016) *Cybernauci – diagnoza wiedzy, umiejętności i kompetencji dzieci i młodzieży, rodziców i opiekunów oraz nauczycieli w zakresie bezpiecznego korzystania z internetu. Raport podsumowujący badanie ex-ante* (Warszawa: Fundacja Nowoczesna Polska), available at: https://www.civitas.edu.pl/wp-content/uploads/2016/06/Raport-v.6.1.pdf (September 19, 2021).

Blake, W. (1994) *Wiersze i poematy* (Warszawa: Świat Literacki).

Castells, M. (2013) *Władza komunikacji* (Warsaw: Wydawnictwo Naukowe PWN).

Chałubińska-Jentkiewicz, K. (2019) *Cyberodpowiedzialność* (Toruń: Wydawnictwo Adam Marszałek).

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2021) *Ochrona danych osobowych w cyberprzestrzeni* (Warsaw: Akademia Sztuki Wojennej, War Studies University).

Dela, A. (2020) *Teoria walki w cyberprzestrzeni* (Warsaw: Wydawnictwo Akademii Sztuki Wojennej).

Deleuze, G. & Guattrai, F. (1980) *A Thousand Plateau. Capitalism and Schisophrenia* (London: University of Minnesota Press).

Filek, J. (ed.) (2004) *Filozofia odpowiedzialności XX wieku* (Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego).

Fundacja Kronenberga (2020) *Złapani w sieć – Jak Polacy radzą sobie w cyberprzestrzeni*, available at: https://www.citibank.pl/poland/kronenberg/polish/files/Raport-cybersecurity.pdf (September 22, 2021).

Hallowell, J.H. (1993) *Moralne podstawy demokracji* (Warszawa: PWN).

Harwas-Napierała, B. (2005) Etyczne aspekty manipulacji, *Poznańskie Studia Teologiczne*, (18), pp. 247-259.

Heywood, A. (2008) *Klucz do politologii. Najważniejsze ideologie, systemy, postaci* (Warsaw: PWN).

Ingarden, R. (1987) *Książeczka o człowieku* (Kraków: Wydawnictwo Literackie).

Europol (2021) *Internet Organised Crime Threat Assessment (IOCTA) 2020*, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (September 24, 2021).

Krąpiec, M.A. (1991) *O rozumienie filozofii* (Lublin: KUL).

Liddell-Hart, B.H. (1959) *Strategia. Działania pośrednie* (Warsaw: Wydawnictwo Ministerstwa Obrony Narodowej).

Nowicka-Kozioł, M. (1993) *Odpowiedzialność w świetle alternatyw współczesnego humanizmu* (Warsaw: Wydawnictwo WSPS).

Babak, A., Saskia, P., Bayerl, P. & Sampson, F. (eds.) (2016) *Open Source Intelligence Investigation* (New York: Springer).

Patrick, J.J. (2018) *The Art of Hybrid War* (London: Cynefin Road).

Robertson, D. (2009) *Słownik polityki* (Warszawa: PWN).

Ryszka, F. (1974) *Państwo stanu wyjątkowego* (Wrocław: Zakład Narodowy im. Ossolińskich).

Sartori, G. (2007) *Homo videns. Telewizja i postmyślenie* (Warsaw: Wydawnictwo UW).

Sennet, R. (2010) *Etyka dobrej roboty* (Warsaw: Wydawnictwo Literackie Muza S.A.).

Pawłowski, J., Zdrodowski, B. & Kuliczkowski, M. (eds.) (2020) *Słownik terminów z zakresu bezpieczeństwa* (Toruń: Wydawnictwo Adam Marszałek).

Soler, U. (2015) Technologie sieciowe vs terroryzm – czy mogą być społecznie szkodliwe?, *Zeszyty Naukowe Politechniki Śląskiej*, (85), pp. 495-506.

Strauss, L. (1998) *Sokratejskie pytania* (Warsaw: Fundacja Aletheia).

Świniarski, J. (1999) *Filozoficzne podstawy edukacji dla bezpieczeństwa* (Warsaw: Departament Społeczno-Wychowawczy Ministerstwa Obrony Narodowej).

Taraszkiewicz, B. (ed.) (2014) *Ekologia informacji w e-społeczeństwie* (Słupsk: Stowarzyszenie Bibliotekarzy Polskich - Zarząd Oddziału Słupskiego, Biblioteka Uczelniana Akademii Pomorskiej w Słupsku, Pedagogiczna Biblioteka Wojewódzka w Słupsku), available at: https://depot.ceon.pl/bitstream/handle/123456789/17699/Ekologia%20informacji%20-%20Taraszkiewicz.pdf?sequence=1&isAllowed=y (September 19, 2021).

Tinder, G. (2003) *Myślenie polityczne* (Warsaw: PWN).

Volkoff, V. (1991) *Dezinformacja. Oręż wojny* (Warsaw: Wydawnictwo Delikon).

Zubik, M. (2008) *Wybór dokumentów prawa międzynarodowego dotyczących praw człowieka* (Warsaw: Biuro Rzecznika Praw Obywatelskich).

Cooperation Mechanisms to Ensure the Security of Network and Information Systems in the Light of the NIS Directive

MONIKA NOWIKOWSKA

Abstract In recent years we have seen a spike in interest in cybersecurity, resulting in an increasing number of individuals and organisations being established to deal with this problem. However, in order to carry out public tasks in this area more effectively, it is necessary for particular entities to cooperate and exchange information. Cooperation mechanisms to ensure the security of network and information systems are defined in Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high, common level of security of network and information systems across the Union (OJ EU L 194/1).

Keywords: • network and information systems • cyberspace • public administration • cooperation • single point of contact • CSIRT • Cooperation Group

CORRESPONDENCE ADDRESS: Monika Nowikowska, Ph.D., Assistant Professor, War Studies University in Warsaw, Institute of Law, Department of New Technologies and Cybersecurity Law, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: m.nowikowska@akademia.mil.pl, ORCID: 0000-0001-5166-8375.

https://doi.org/10.4335/2022.2.6 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

In an era of the constant development of new technologies, networks, as well as information, systems and services are essential for any state to operate. Fundamental importance is attributed to the internet, which plays a primary role in facilitating the cross-border movement of goods, services and people. Due to its global, supranational character, the importance of the proper functioning of networks and systems, their reliability and security constitute a *sine qua non* condition for the efficient functioning of states and societies. The scale, frequency and impact of security incidents are becoming more and more important and pose a serious threat to the functioning of network and information systems. These systems may also become an object of intentional harmful actions aimed at damaging or disrupting their operation (Chałubińska-Jentkiewicz, Nowikowska, 2020:305).

Furthermore, public authorities have been obliged to provide citizens with electronic services covering both the handling of citizen matters and other areas of public administration operation. The processes of the computerisation of public administration are accompanied by changes related to the mode of operation in the state-citizen relationship (Chałubińska-Jentkiewicz, 2019:68). Thus, IT services have become an essential tool to ensure the efficiency of administrative apparatus (Knosala, Matan, Zacharko, 1999:126).

In order to promote and facilitate strategic cooperation between states on the security of network and information systems at the European Union level, the European Parliament and the Council of the European Union adopted on 6 July 2016 Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the so-called NIS Directive) (OJ EU L194/1). The preamble of the NIS Directive indicates that the existing capabilities are not sufficient to ensure a high level of security of network and information systems. Member States have very different levels of preparedness, which has led to fragmented approaches towards the issues related to the security of network and information systems across the Union. In consequence, this may result in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Similarly, a lack of common requirements on the operators of essential services and digital service providers makes it impossible to set up a global and effective mechanism for cooperation between Member States. Thus, in order to respond effectively to the challenges of the security of network and information systems, a decision was made to adopt a global approach at the Union level covering i.e., common minimum capacity building and planning requirements, the exchange of information, cooperation and common security requirements for operators of essential services and digital service providers.

As a consequence of the adoption of the NIS Directive and for the purpose of establishing a coherent system to ensure cybersecurity of the Republic of Poland, on 5 July 2018 the Sejm of the Republic of Poland enacted the Act on the National Cybersecurity System, which entered into force on 28 August 2018. The said Act and the accompanying implementing regulations have fully implemented the provisions of the NIS Directive into the Polish legal order.

The subject matter of this paper are the mechanisms of cooperation to ensure the security of network and information systems in the light of the NIS Directive. This topic required an analysis of the content and evaluation of the source literature (using the *desk research* technique) and of the selected EU and Polish legal acts, covering three fundamental issues: the concept of network and information systems, the concept of cyberspace and the *ratio legis of* establishing cooperation mechanisms to ensure the security of network and information systems.

2 The concept of network and information systems

The concept of network and information systems is defined in Article 4 of the NIS Directive. According to that provision, "network and information systems" means: a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24/04/2002) b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

Within the meaning of Article 2(a) of Directive 2002/21/EC (a) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

The Union legislator also chose to define the "security of network and information systems", which means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

It should be noted that this definition is consistent with the definition of information security contained in ISO/IEC 27001:2005 and ISO/IEC 17799:2007. The ISO/IEC 17799:2007 Guide to Information Security Management System defines information security as the preservation of information properties, i.e., *confidentiality*, *integrity*, *availability*, *accountability*, *authenticity*, *non-repudiation* and *reliability*. The first three properties - confidentiality, integrity and availability – form the backbone for building an information security system. Their importance varies from organisation to organisation. For government institutions, confidentiality is important. For organisations producing statistical research, the most important property will be integrity during data processing. These entities must not make any mistakes, as this can have a very negative impact on their credibility. Availability, on the other hand, is the most important condition for all entities in the service industry, where any short interruption in business operations can result in exponential financial loss (Łuczak, Tyburski, 2009:12). Information confidentiality, integrity, availability, accountability, authenticity, non-repudiation and reliability are the so-called attributes of information security (Chałubińska-Jentkiewicz, Nowikowska, 2020:34).

Confidentiality *means ensuring that information is only accessible to authorised persons with the appropriate right of access.* In other words, confidentiality can be construed as the ability to make information available for common use by many people, while at the same time not making it available to those who should not read it. *Maintaining confidentiality is present to prevent the detection of the source of transmission*, data *destination*, frequency, length and other transmission characteristics. Loss of confidentiality may occur during information handling, for instance while copying it. Despite various measures to ensure confidentiality, there is a risk of accidental or intentional breaches of confidentiality. Therefore, a security system should not only ensure confidentiality, but also guarantee the possibility of detecting attempts to breach confidentiality and the breaches themselves. A fundamental aspect for maintaining confidentiality is to define a closed list of persons, the so-called depositaries, who can read the information. The ability of an organisation to maintain confidentiality is essentially based on the management of classified information. Once an organisation has identified any specific information that requires confidentiality protection, it is possible to introduce rules and methods for handling the given information. This primarily concerns: the marking of information and the rules for its copying, storage, destruction, and sharing (Łuczak, Tyburski, 2009:13).

Integrity means the tracking of information processing in all its forms to prevent unauthorised modification, or to eliminate an incorrect processing method. We can speak of maintaining the integrity of information when any intentional or unintentional unauthorised modification of information is impossible. Ensuring integrity is essential when it is possible for the user to modify data in a way that may cause the information to be false, incomplete or falsified. A key aspect for maintaining integrity is access control.

This means ensuring that information is created or updated in a controlled manner and is protected against damage or destruction.

Availability, on the other hand, means the assurance that information is available to an authorised person at any time that that person may need it. The loss of availability as one of the properties of information security may lead, most often, to a loss of business continuity, and thus productivity. It may result in a loss of income, as well as generate direct or indirect financial losses. Lack of access to a specific piece of information may result in an organisation failing to complete its tasks on time. Considering the equipment that supports an information system, it should be designed in such a way so as to ensure its high availability and redundancy of all major components, including disk drives, power supplies, fans, etc., so that repairing a failed component should not cause any downtime. It is the infrastructure that modern information systems rely on. The two most important infrastructure components are power supply and telecommunications. The availability of power or the elimination of interruptions in supplying information systems with power is deemed to be a basic need. Uninterruptible power supplies and backup generators provide power in the event of an interruption. Network availability is based on redundancy in networks and multiple supplies, making the network even more accessible. In addition, it is necessary to ensure the possibility to repair and replace any part of this system without causing significant downtime of equipment in contact with information. This will guarantee optimum performance and minimum impact due to any damage. A system that remains available should be equipped with a real-time backup function. Such a solution will enable access to the latest data, even in the case of any unintentional loss of information by an employee. Availability in organisations hinges primarily on the ability to avoid or overcome the factors that cause downtime, or on the ability to quickly remove downtime (Łuczak, Tyburski, 2009:15).

Therefore, the basic components of information security are: information security management, network security, policy, data and computer security (Chalubinska-Jentkiewicz, Nowikowska, 2020:36).

Under Polish law, the terminology relating to the network and information system notions analysed herein is not uniform, which causes a number of controversies. Particular normative acts use different concepts, such as: information systems (*systemy informacyjne)*, IT systems *(systemy informatyczne)*, and communication and information systems (*systemy teleinformatyczne*), which may be mistakenly treated as synonyms. In 2016, the term "information system" appeared in 390 acts published in the Journal of Laws, "IT system" – in 1242 and "communication and information system" – in 1138 (Szpor, 2016:120). In order to discuss the issue of cooperation mechanisms to ensure security in cyberspace, it seems necessary to put the terminology discussed herein in order.

Information systems is a legal term that appeared in the 1990's, among others in the Act of 29 June 1995 on Official Statistics (Journal of Laws of 2021, item 955). The notion of public administration information systems covers systems for collecting, gathering and processing information by public administration bodies, the Social Insurance Institution (ZUS), the National Health Fund, the Financial Supervision Authority (KNF), registration bodies, other legal bodies of the state or local government, as well as other entities keeping official registers (Article 2(13)).

IT system is defined, among others, in the Act of 24 August 2007 on the Participation of the Republic of Poland in the Schengen Information System and the Visa Information System (Journal of Laws of 2021, item 1041)."IT system" is construed as a set of cooperating devices, information processing procedures and SW tools (software) used for data processing, along with the telecommunication infrastructure enabling public administration bodies and justice administration bodies to process the data collected in the Schengen Information System and the Visa Information System.

In the source literature an IT system is construed as a device or a group of interconnected or related devices (i.e., hardware), such as a processor or a central processing unit together with the peripheral devices connected thereto (monitor, printer, etc.), if any, as well as the software enabling automatic data processing. Hence, it will be a mobile phone or a personal computer (Radoniewicz, 2019:46).

Communication and information system is a term that appears, among others, in the regulation on the protection of classified information. A communication and information system is defined in Article 2(6) of the Act of 5 August 2010 on the Protection of Classified Information (Journal of Laws of 2019, item 1228). "Communication and information system" shall be construed as defined in Article 2(3) of the Act of 18 July 2002 on the Provision of Services by Electronic Means (Journal of Laws of 2020, item 344). Since the legislator made reference to another act, a communication and information system on the grounds of protection of classified information means a set of cooperating IT devices and software, ensuring processing and storing, as well as sending and receiving data through telecommunications networks by means of terminal equipment appropriate for the given type of network, within the meaning of the Act of 16 July 2004 – Telecommunications Law (Journal of Laws of 2021, 576). The source literature indicates that a photocopier is a communication and information system – within the meaning of the Act of 5 August 2010 on the Protection of Classified Information – which makes it possible to prepare and store classified information on a computer data carrier (Anzel, 2018:73). It seems that the term "communication and information system" emphasises the connection with telecommunications, which is currently defined by law as the emission, reception or transmission of information, irrespective of its type, by wire, radio, optical or other electromagnetic means.

On the other hand, telecommunications network, according to Article 2(35) of the Telecommunications Law, means transmission systems and switching or routing equipment as well as other resources, including non-active network elements, which enable the emission, reception or transmission of signals by wire, radio, optical or other electromagnetic means, irrespective of their type; (Krupa, 2020:183).

To summarise the above, it should be stated that an interdisciplinary agreement on the relations between the concepts of "communication and information system", "IT system" and "information system" is desirable. Under the NIS Directive, the legislator used the term *information system*, which was translated into Polish as *systemy informatyczne* (IT systems). In view of the fact that the term "information systems" is often used in the Polish legal language, where the term is generally construed as cooperating devices, information processing procedures and SW (software) tools used for the purpose of data processing, and the telecommunications infrastructure enabling the processing of collected data, using this very term seems appropriate. It includes both technical infrastructure and information resources (*content)*. The term "IT systems" used in the Polish version of the Directive may lead to a narrowing of the meaning of this concept to hardware and software, marginalising the importance of security of the content processed in IT systems.

3 Concept of cyberspace

Under both Union law and Polish legislation, there is no single legal definition of cyberspace. It is an underspecified concept. There is also no universally accepted definition of cyberspace. The term *cyberspace* originates from the combination of two words: *cybernetics* and *space*, which means cybernetic space. The term emerged in the 1980's. It is believed to have been coined by the Canadian writer W. Gibson in his 1984 novel "Neuromancer" to describe the computer-generated virtual reality in which his protagonists found themselves. The term has permeated into mass culture and is now used primarily to describe virtual space, i.e. the space of communication via computer networks (Radoniewicz, 2019:33).

In Polish law the term appears in various acts which give an autonomous meaning to the term "cyberspace". For example, in Article 2(1a) of the Act of 18 April 2002 on the State of Natural Disaster (Journal of Laws of 2017, item 1897), cyberspace is construed as the space for the processing and exchange of information created by communication and information systems, as defined in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (Journal of Laws of 2021, item 670), together with their mutual interrelations and interactions with users. A communication and information system, within the meaning of the Act on the Computerisation of the Operations of the Entities Performing Public Tasks, is a set of IT devices and software, ensuring processing and storing, as well as sending and receiving data through telecommunications networks by means of terminal equipment appropriate

for the given type of network (Czarnecka, 2019:67). The term “cyberspace” understood in this way has also been repeated in the Act of 29 August 2002 on the Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland in Article 2(1b) thereof (Journal of Laws of 2017, item 1932) and the Act of 21 June 2002 on the State of Emergency in Article 2(1a) thereof (Journal of Laws of 2017, item 1928). Thus, as it stems from this relatively broad definition, the legislator construes cyberspace not only as communication and information systems, i.e. the devices (hardware) they consist of, together with the programs (software) ensuring the performance of functions by these systems (processing, storage and transmission of computer data), but also as computer data (information) and interactions between devices and their users (see more broadly Aleksandrowicz, Liedel, 2012:23; Liderman, 2017:62-63).

To sum up the foregoing, it can be stated that in accordance with the definition of cyberspace adopted under the acts on extraordinary states it contains both the term “information” and the term “communication and information systems”, which terms are the core of the definition of cyberspace. Given the use of the expressions "mutual interrelations" (relations between communication and information systems) and "relations with users", which are not catalogued by the legislator, one may try to argue the definition of cyberspace is a type of definition whose scope is incomplete. By design, incomplete definitions do not list all elements of the scope, but limit themselves only to highlighting an example of these elements (Taczkowska-Olszewska, 2019:4). However, this observation may also lead to the opposite thesis, according to which a rational legislator did not concretise the types and features of the said relations existing between subjects (users) of cyberspace, intending to achieve the goal of covering all types of activity with this term, regardless of the status of any subjects, time, place or purpose of undertaking it, with the reservation that this activity takes place with the use of communication and information systems, and its object is information (Taczkowska-Olszewska, 2017:53).

In the source literature, M. Lakomy emphasises that cyberspace is a global information infrastructure, the interconnectivity between people by means of computers and telecommunications (Lakomy, 2015:67). Similarly, P. Levy notes that cyberspace is an information domain, a space for open communication through computers around the world (Levy, 2002:380).

The analysis of doctrinal definitions of cyberspace allows us to identify certain elements characteristic of the cyberspace environment. They include: 1) unlimited reach; 2) the welding of information resources into huge databases; 3) no possibility to reference cyberspace to the physical dimensions of the real world (Wasilewski, 2013:226), 4) the complexity of the phenomenon, by basing cyberspace on technical, technological and social elements (Dobrzeniecki, 2004:21), 5) the combination of communication and

information systems, information and interactions between devices and their users (Radoniewicz, 2019:49).

The need to take action to determine the standard norms, principles and values in cyberspace was indicated by the European Commission in its Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace" (EU Commission Communication of 7.2.2013, JOIN(2013), 1 final) – hereinafter the Communication. In this Communication, the Commission stressed that fundamental rights, democracy and the rule of law need to be protected in cyberspace. Freedom in the online environment requires safety and security. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace, whose mission should be to respect and protect fundamental rights online and to maintain the reliability and interoperability of the internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative in this area has to recognise its leading role (Chalubinska-Jentkiewicz, Nowikowska, 2020:21).

One of the key regulatory objectives is to ensure cybersecurity, which requires actions related to maintaining the availability and integrity of networks and infrastructure, as well as the confidentiality of any information contained therein, subject to the right of privacy and with respect for identity. Ensuring cybersecurity becomes one of the fundamental objectives of the State, and the determinant of these principles is the protection of fundamental values, which should have the same degree of protection in cyberspace as in the real world. Cyberspace that is open and free removes social and international barriers, allows the exchange of cultures and experiences between states, communities and individuals, enabling interactions and the exchange of information, and consequently the exchange of knowledge, experience and technology.

The way in which cyberspace is defined, as well as the place in a system of legal acts in which this definition is placed, determine both the need for inseparable protection of the content of information and the methods of its transmission, recording, generation and storage, as well as – on the other hand – the rank of information in the hierarchy of legally protected interests. The rank of information has increased. Not only because in the era of an information society it has become a factor of the economic growth of states, but mainly down to the value of information as a new kind of weapon and a tool of war used in a new arena of the fifth theatre of war, besides land, air, water and space, which cyberspace has become (Chalubinska-Jentkiewicz, Karpiuk, 2015:57; Liedel, 2011:48; Lakomy, 2015:63). It is de facto synonymous with “information space” construed as aggregated information resources available to an individual with the use of communication and information systems. Therefore, cyberspace can be seen as "the space of information created by all computer networks put together" (Denning, 2002:25).

4 Cooperation mechanisms

In order to respond effectively to the challenges of ensuring the security of network and information systems in cyberspace, the EU legislator has indicated the need to build a common, comprehensive approach, covering, among others, the exchange of information and cooperation between Member States.

An analysis of the provisions of the NIS Directive makes it possible to distinguish cooperation mechanisms at two levels: 1) a technical level and 2) a political and strategic level.

Cooperation in technical terms is to be ensured through a European CISRT network and the creation of mechanisms for the exchange of information on cross-border incidents between CSIRTs designated for operators of essential services and digital service providers.

Cooperation in the political and strategic dimension is to be implemented through the establishment of a Cooperation Group, which will develop joint strategic conceptions and receive, inter alia, annual reports from competent authorities.

The Directive did not determine the precise mechanisms of operation in the two fora. Both the CSIRT Network and the Cooperation Group are to define them themselves.

In order to be able to cooperate effectively with economic actors, Member State bodies need to be structured accordingly. Hence, the NIS Directive distinguishes between points of contact and the computer security incident response teams (called "CSIRTs"). The single points of contact should not directly receive any notifications of incidents. This task belongs to the CSIRTs. The designated point of contact is however required to forward incident notifications to the single points of contact of other affected Member States. To ensure the effective provision of information to the Member States and to the Commission, a summary report should be submitted by the single point of contact to the Cooperation Group, and should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and digital service providers, as information on the identity of the notifying entities is not required for the exchange of best practice in the Cooperation Group. The summary report should include information on the number of notifications received, as well as an indication of the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.

Recital 31 of the NIS Directive stipulates that in order to facilitate cross-border cooperation and communication, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at the Union level.

Competent authorities and single points of contact should have the adequate technical, financial and human resources to ensure that they can carry out the tasks assigned to them in an effective and efficient manner and thus achieve the objectives of this Directive.

The Single Point of Contact serves communication within the European Union. The exchange of information between EU Member States serves the implementation of objectives of the NIS Directive in terms of achieving a high common level of security of network and information systems in the Union. Under the Polish Act on the National Cybersecurity System, the Single Point of Contact shall forward, at the request of the competent CSIRT MON, CSIRT NASK or CSIRT GOV, notifications of a serious or significant incident concerning two or more EU Member States to the Single Points of Contact in other EU Member States. It is also required to receive notifications of a serious incident concerning two or more European Union Member States from the Single Points of Contact in other European Union Member States and then forward these notifications to the CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams (Chalubinska-Jentkiewicz, 2019:296).

When implementing the NIS Directive, the Polish legislator assumed that the Minister for Computerisation, acting as the Single Point of Contact, is responsible for receiving and forwarding, at the request of relevant CSIRTs, notifications of a serious or significant incident concerning two or more Member States of the European Union. Moreover, it is responsible for ensuring the representation of the Republic of Poland in the Cooperation Group, the exchange of information for the benefit of public authorities, competent authorities in Poland and abroad, CSIRT and the fulfilment of reporting obligations towards the Cooperation Group and the European Commission.

The main tasks of the point of contact include: 1) receiving reports of a serious or significant incident concerning two or more Member States of the European Union from single points of contact in other Member States of the European Union, as well as forwarding these notifications to the CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams - i.e. acquiring and forwarding information on any existing emergency situation from other points of contact in the EU, if the situation there is of a broader character, because it concerns more than one state; 2) forwarding, at the request of the competent CSIRT MON, CSIRT NASK or CSIRT GOV, notifications of a serious or significant incident concerning two or more Member States of the European Union to single contact points in other Member States of the European Union - i.e. acquiring and forwarding information about such incidents to other points of contact, which are affected by the incident 3) ensuring representation of the Republic of Poland in the Cooperation Group - i.e. fulfilling a representative function; 4) ensuring cooperation with the European Commission in the area of cybersecurity - i.e. fulfilling the policy of cooperation with the EU in the area of cybersecurity 5) coordinating cooperation between the competent authorities for cybersecurity and public authorities in the Republic of Poland with the relevant authorities in the European Union member states - i.e. coordinating the

cooperation between the state and other EU states on cybersecurity; 6) ensuring the exchange of information for the needs of the Cooperation Group and the CSIRT Network - i.e. implementing information aspects of cooperation (Chalubinska, 2019:296-297).

Cooperation in the political and strategic dimension is implemented through the establishment of the Cooperation Group. The Cooperation Group - as an auxiliary tool for assessing national strategies for the security of network and information systems - should serve as a tool for exchanging best practices, discussing capabilities and preparedness of the Member States. The tasks of the Cooperation Group also include assisting the Member States in evaluating national strategies on the security of network and information systems, building capacity and evaluating exercises relating to the security of network and information systems. Furthermore, in order to promote advanced security of network and information systems, the Cooperation Group should, where appropriate, cooperate with relevant Union institutions, bodies, offices and agencies, to exchange know-how and best practices, and to provide advice on security aspects of network and information systems that might have an impact on their work, while respecting existing arrangements for the exchange of restricted information. In cooperating with law enforcement authorities regarding the security aspects of network and information systems that might have an impact on their work, the Cooperation Group should respect existing channels of information and established networks (Chalubinska-Jentkiewicz, 2019:298). In order to carry out the tasks of the Cooperation Group, the single points of contact must provide it with specific information. This is because a key element in activities related to ensuring cybersecurity is information policy.

Also noteworthy is the cooperation of the Polish Armed Forces with international bodies in the area of cybersecurity, as regulated in the Act on the National Cybersecurity System. The task defining the order of cooperation of the Armed Forces of the Republic of Poland with the relevant bodies of the North Atlantic Treaty Organisation, the European Union and international organisations in the area of national defence in the field of cybersecurity definitely requires the Minister of National Defence to look for the legal norms clearly indicated in universally binding regulations which provide for competence of this body to implement such a generally outlined task. In Article 51 of the Act on the National Cybersecurity System, the legislator indicated that the cooperation of the Armed Forces of the Republic of Poland with the relevant bodies of the North Atlantic Treaty Organisation, the European Union and international organisations in the area of national defence in the field of cybersecurity is the responsibility of the Minister of National Defence.

5 Summary

The purpose of providing information about CSIRT tasks, including the main elements of incident handling procedures, is to build a common and uniform cybersecurity system. Cooperation is widely defined as performing certain activities together with someone.

Simultaneously, the essence of relationships between individuals, defined as cooperation, is striving for a common goal or helping each other to achieve divergent goals. Cooperation means positive collaboration aimed at the achievement of the effect of synergy.

Under the NIS Directive, a system of the so-called points of contact has been designed to implement cooperation in cyberspace. Pursuant to Article 8(3) of the NIS Directive, each Member State shall designate a national single point of contact on the security of network and information systems. In Polish conditions, such a body is the Minister for Computerisation. Pursuant to Article 8(4) of the NIS Directive, the single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group and the CSIRTs network. At the same time, under Article 11 of the NIS Directive, the Union legislator has indicated the need to establish a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States, and to achieve a high, common level of security of network and information systems in the Union. Thus, based on an analysis of the provisions of the NIS Directive one may distinguish the cooperation to ensure the security of network and information systems on two levels: a technical level, through the establishment of the CISRT and mechanisms for the exchange of information on cross-border incidents, and a political and strategic level, realised through the establishment of the Cooperation Group.

References:

Aleksandrowicz, T.R. & Liedel, K. (2012) *Analiza informacji. Teoria i praktyka* (Warsaw: Difin Publishing House).

Anzel, M. (2018) Urządzenia teleinformatyczne a sporządzanie i przechowywanie informacji niejawnych, *Informacja w Administracji Publicznej*, (3), p. 73.

Banasiński, C. (2018) Podstawowe pojęcie i podstawy prawne bezpieczeństwa w cyberprzestrzeni, In: Banasiński, C. (ed.) *Cyberbezpieczeństwo* (Warsaw: Wolters Kluwer Publishing House), pp. 22-65.

Chałubińska-Jentkiewicz, K. & Karpiuk, M. (2015) *Prawo nowych technologii. Wybrane zagadnienia* (Warsaw: Wolters Kluwer Publishing House).

Chałubińska-Jentkiewicz, K. (2019) Cyberodpowiedzialność (Toruń: Wydawnictwo Adam Marszałek).

Kitler, W., Taczkowska-Olszewska, J. & Radoniewicz, F. *Ustawa o krajowym systemie cyberbezpieczeństwa* (Warsaw: C.H. Beck Publishing House), pp. 48, 297-297.

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2020) *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne* (Warsaw: C.H. Beck Publishing House).

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2020) *Ochrona informacji w cyberprzestrzeni* (Warsaw: Akademia Sztuki Wojennej Publishing House).

Czarnecka, A. (2019) Wybrane obowiązki operatorów usług kluczowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa, *Informacja w administracji publicznej*, (2), pp. 64-69.

Denning, D.D. (2002) *Wojna informacyjna i bezpieczeństwo informacji* (Warsaw: Wydawnictwo Naukowo Techniczne), p. 25.

Knosala, E., Matan, A. & Zacharko, L. (1996) *Zarys nauki administracji* (Katowice: Wydawnictwo Uniwersytetu Śląskiego).

Krupa, W. (2020) Kwalifikacja działalności podlegającej obowiązkowi wpisu do rejestru przedsiębiorców telekomunikacyjnych, *IUS NOVUM*, 14(4), pp. 181-204.

Lakomy, M. (2015) *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw* (Katowice: Wydawnictwo Uniwersytetu Śląskiego), p. 63.

Liderman, K. (2017) *Bezpieczeństwo informacyjne, Nowe wyzwania* (Warsaw: PWN Publishing House), pp. 62–63.

Liedel, K. (2011) *Transsektorowe obszary bezpieczeństwa narodowego* (Warsaw: Difin Publishing House), pp. 48-48.

Radoniewicz, F. (2019) Komentarz, In: Kitler, W., Taczkowska-Olszewska, J. & Radoniewicz, F. (eds.) *Ustawa o krajowym systemie cyberbezpieczeństwa* (Warsaw: C.H. Beck Publishing House), pp. 48, 297-297.

Szpor, G. (2017) *Jawność i jej ograniczenia, Tom I. Idee i pojęcia* (Warsaw: C.H. Beck Publishing House), pp. 120-124.

Taczkowska-Olszewska, J. (2017) Bezpieczeństwo informacyjne jako kategoria prawna. Ujęcie teoretyczne, In: Kitler, W. & Taczkowska-Olszewska, J. (eds.) *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne* (Warsaw: Towarzystwo Wiedzy Obronnej Publishing House), pp. 53.

Taczkowska-Olszewska, J. (2019) Pojęcie cyberprzestrzeni, In: Taczkowska-Olszewska, J., Chałubińka-Jentkiewicz, K. & Nowikowska, M. (eds.) *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa* (Warsaw: C.H. Beck Publishing House), pp.3-9.

New Obligations of Telecommunication Entrepreneurs Under the Draft Act Amending the National Cybersecurity System Act and the Telecommunications Law Act

KAROLINA GRENDA

Abstract The National Cybersecurity System Act adopted in 2018 unquestionably laid the legal and institutional groundwork for the development of a cybersecurity system at the state level. From a practical point of view, the direct reason for the initiation of the work on amendments to the law was, primarily, the lack of sectoral team appointment, despite the possibility provided by law. The regulations in question are intended to improve the effectiveness of incident response by the appointment of a CSIRT for each sector. The primary objective of telecommunications enterprises is to ensure the security and integrity of networks, services and communication transmission, as well as to protect the substance and functionality of the network and its ability to provide services. Measures preventing threats to the network, services and communications are of fundamental importance.

Keywords: • cybersecurity • CSIRT • telecommunications enterprise

CORRESPONDENCE ADDRESS: Karolina Grenda, Ph.D. student, SWPS University of Social Sciences and Humanities in Warsaw, Institute of Law, Chodakowska 19/31, 03-815 Warszawa, Poland, e-mail: karolina.mielnik@gmail.com.

https://doi.org/10.4335/2022.2.7 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

The government draft act of 20 January 2021 amending the National Cybersecurity System Act and the Telecommunications Law Act (originally, the draft was named – "on amending the National Cybersecurity System Act and the Public Procurement Law Act") was communicated in the Public Information Bulletin on the website of the Government Legislation Centre, on 7 September 2020, thus formally initiating the process of its approval. The fact that the works on the draft took more than one year (as of 30 August 2021, the draft amending the act was still in the works at the Government Legislation Centre) and the scope of changes introduced reflect the importance and complexity of its subject matter.

The Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws of 2018, item 1560, as amended) ("NCSA"), which is a legislative initiative of the government, implemented into the national legal framework the provisions of Directive 2016/1148 of the European Parliament, and of the Council (EU) concerning measures for a high common level of the security of network and information systems across the Union (Directive 2016/1148 of the European Parliament, and of the Council (EU), of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union (Official Journal EU L 194 of 19 July 2016, p. 1) ("NIS"); however, its primary purpose was to organise and implement in legal and functional terms the national cybersecurity system.

Until the entry into force of the Act, the issues concerning securing ICT systems were regulated separately for each sector or area. The measures used to ensure information security management in public entities (Regulation of the Council of Ministers of 12 April 2012 on the National Interoperability Framework (KRI), the minimum requirements for public records and the exchange of information in electronic form, and the minimum requirements for communication and information systems (Journal of Laws of 2017, item 2247), counteracting cybercrime and preventing terrorist threats (the Act of 10 June 2016 on Anti-Terrorism (Journal of Laws of 2018, items 452, 650 and 730, as amended)), crisis management (the Act of 26 April 2007 on Crisis Management (Journal of Laws of 2017, items 209 and 1566, as amended)), as well as regulations concerning such issues as securing services provided by telecommunications enterprises (the Telecommunications Law Act of 16 July 2004 (Journal of Laws of 2019, items 1907 and 2201 and of 2018, items 106, 138 and 650, as amended)) or banks (the Act of 29 August 1997 – Banking Law (Journal of Laws of 2017, items 1876, 2361 and 2491 and of 2018, items 62, 106, 138, 650, 685 and 723) were ineffective. None of the existing solutions, prior to the adoption of the Act, addressed the problem in a comprehensive manner. No commonly applicable regulations were in force in Poland that would specify the detailed scope of the authorities' power in the area of cybersecurity with regard to the sectors indicated in the Directive.

The National Cybersecurity System Act adopted in 2018 unquestionably laid the legal and institutional groundwork for the development of a cybersecurity system at the state

level. A competent authority for cybersecurity was established for each sector, which is now responsible for the designation of operators, the supervision and monitoring of compliance with the provisions of the Act in each respective sector. As a result of the adoption of this regulation, works were also commenced to create the structures of the national cybersecurity system. The experience gained during the two years of its implementation pointed to the need for changes at the statutory level.

As stated in its rationale, the draft act amending the National Cybersecurity System Act is to serve the objective of the Cybersecurity Strategy of the Republic of Poland for 2019-2045 (Resolution No. 125 by the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019-2024 (Official Gazette of the Government of the Republic of Poland of 2019, item 1037), which is to increase resilience to cyber threats and enhance information protection in the public, military and private sectors. It also serves the specific objective consisting in the development of the national cybersecurity system by evaluating existing cybersecurity legislation.

From a practical point of view, the direct reason for the initiation of the work was, primarily, the lack of sectoral team appointment, despite the possibility provided by law. The regulations in question are intended to improve the effectiveness of incident response by the appointment of a CSIRT for each sector. In the opinion of the legislator, this change will allow the operators of essential services to deal with incidents in a faster and more effective way. There is also a related proposal to change the name of the sectoral cybersecurity team to the sectoral CSIRT. In contrast to the currently practised optional mode of team appointment, the draft provides for the mandatory appointment of a CSIRT for each sector or sub-sector by a competent authority. The aim of the legislators is to impose on the sectoral CSIRT the responsibility for receiving and handling incident reports in the relevant sector or sub-sector, as well as dynamic risk analysis and the collection of information on cyber threats. Currently, the role of the sectoral cybersecurity team is limited to supporting digital service operators in responding to incidents.

The draft recognises the need to increase the powers of the Government Plenipotentiary for Cybersecurity (Plenipotentiary), which is also expected to support the strengthening and coordination of cooperation between the entities within the national cybersecurity system and provide a more effective response to new threats. One of the most common problems is the lack of appropriate structures of the operators of essential services, as well as a shortage of skills and a decreased awareness of cyber threats, which hinders an effective response to security incidents.

The amendment is designed to improve cooperation between the entities responsible for cybersecurity at the provincial level. For this purpose, it introduces procedures for cooperation between public entities operating in this area. During the audits conducted by the Supreme Audit Office in 2019 (Supreme Audit Office, 2019), irregularities were

found in the performance of tasks related to ensuring the security of information processing in 70% of the audited local government units. The coordination of tasks at the provincial level is expected to facilitate the exchange of information on cyber threats, which is also important from the perspective of local government units, which, in 2015, as a result of the entry into force of the System of State Registers (SRP), were entrusted with most of the tasks related to its operation. The System of State Registers (SSR) includes the PESEL Register, the Register of Personal Identity Cards and the Database of Civil Registry Office Services. Through access to a dedicated application, it provides services to residents of individual communes related to issuing identity cards, civil registry records, issuing certificates from the above-mentioned registers and keeping registers of residents. In the SSR, the data of all the citizens of Poland is entered and processed.

Since access to expert knowledge on cyber threats is essential for the internal security of the state, the draft act provides for the establishment of the so-called Centres of Information Exchange between the entities within the national cybersecurity system. The purpose of the proposed solution is to collect information on vulnerabilities and threats to information security in one place and to develop good practices, which have not been implemented at the national level so far. The draft predicts that the Centres for Sharing and Analysis of Information, as sectoral or domain-specific initiatives, will be tasked with supporting entities within the national cybersecurity system. The legislative work has led to a proposal to define and introduce into the national cybersecurity system the concept of security operations centres (SOC), which will replace the previous structures responsible for cybersecurity by operators of essential services. As rightly stated, SOCs are well-established structures on the market, fulfilling all functions related to cybersecurity monitoring and management, both in their internal structure and through services provided to other entities. Operators of essential services will establish SOC structures internally or conclude agreements with an external provider of such services. The SOC will perform risk assessments as well as detect and respond to incidents. The list of security operations centres will be kept by the Minister competent for digitisation.

Since resilience to cyber threats depends largely on the security of hardware, software and services, it therefore also applies to ICT systems, telecommunication networks and industrial automation. In accordance with the assumptions of the project, the assessment of risk profiles of hardware or software suppliers will be carried out by the College for Cybersecurity (an entity within the national cybersecurity system referred to in Article 4(20) of the Act on the National Cybersecurity System of 5 July 2018) at the request of its members. When managing risks in their respective information systems, entities within the national cybersecurity system will be obliged to take into account the results of the risk assessments of hardware and software suppliers; they will not be able to use hardware, software and services that pose a high risk and – if currently used – they will have to withdraw them within the time limit specified in the act. The Plenipotentiary's task will be to announce risk assessments in the Official Gazette of the Government of

the Republic of Poland. New powers of the Plenipotentiary will also include issuing security warnings.

Originally, the draft act envisaged including telecommunications enterprises in the scope of the Act. The draft act includes regulations concerning the obligations of telecommunications operators and trust service providers with regard to ensuring cybersecurity. The NIS Directive provides for an exemption in this respect. Pursuant to Article 1 of the aforementioned Directive, the regulations concerning security and incident reporting do not apply to telecommunications enterprises which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Official Journal EU 2002 L 108/33) (the "Framework Directive") nor to trust service providers that are subject to the requirements of Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Journal EU 2014 L 257/73). Currently, the national cybersecurity system covers six sectors of key importance for the socio-economic security of the state and citizens (energy, transport, digital infrastructure, health, banking, water supply). After the amendment, it was to include a new area of electronic communication entrepreneurs, in particular telecommunications entrepreneurs providing services in nationwide networks.

Pursuant to Article 1 of the draft act of 7 September 2020 on amending the Act on the national cybersecurity system and the Act of 29 January 2004 – Public Procurement Law, in Article 1(1), after point three of the Act of 5 July 2018 on the national cybersecurity system (Journal of Laws of 2020, item 1369), point four was added, incorporating into the scope of the subject matter of the Act the tasks and obligations towards electronic communication entrepreneurs referred to in the Act – Electronic Communications Law with regard to security requirements and incident reporting, while in Article 1(2) of the NCSA, it was proposed to repeal points 1 and 2 excluding from the current scope of the NCSA telecommunications entrepreneurs referred to in the Telecommunications Law Act of 16 July 2004 (Journal of Laws of 2017, items 1907 and 2201 and of 2018, items 106, 138, 650 and 1118), with regard to security and incident reporting requirements, and trust service providers who are subject to the requirements of Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ EU L 257 of 28 August 2014, p. 73). In Article 2 of the draft act, it was proposed to add point 3b) to the glossary, defining CSIRT Telco (Computer Security Incident Response Team for electronic communication entrepreneurs). The alignment of requirements with the telecommunications sector under the National Cybersecurity System Act was aimed at ensuring a more effective protection

of essential services provided by entities in other sectors, which – to a large extent – depend on uninterrupted and secure telecommunications services.

The intention of the legislators was for the national cybersecurity system to include electronic communication entrepreneurs, currently excluded from its scope (proposal to repeal Article 1 (2)(1), which excluded the application of the act to telecommunications entrepreneurs. Article 2 of the NCSA contains a glossary of terms used in the act, where point 3a of the definition of CSIRT Telco was added. This would allow to provide them with support in the area of broadly defined incident response. In order to strengthen the situational awareness of national-level CSIRT teams and improve the coordination of incident responses, it was planned to include in the glossary a new category of incident – telecommunication incident. The appointment of a separate CSIRT Telco, whose tasks were to be analogous to the tasks of sectoral CSIRTs, was to provide support for electronic communication enterprises. The management of CSIRT Telco was to be entrusted to the minister competent for computerisation. In order to ensure consistency of the legal system, the amendment initially referred to the definitions of an electronic communications entrepreneur, the provision of a telecommunications network, electronic communication services, telecommunications terminal devices and special risk situations contained in the Act – Electronic Communication Law.

Following the approach adopted in Directive 2016/1148, the current provisions of the NCSA do not apply to telecommunications enterprises and trust service providers who are subject to European and state sectoral requirements on cybersecurity (in Article 1(2) of the NCSA, three exclusions from the application of the act are introduced).

However, the initially planned inclusion of telecommunications enterprises in the subjective scope of the act met with numerous negative opinions during consultations concerning the draft act, both from representatives of academia and government administration, mainly due to potential inconsistency with the NIS Directive. The security requirements provided for in Article 14 do not apply to providers of trust services or enterprises providing public communications networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC; the said enterprises must satisfy the specific requirements in terms of security and integrity set out in Articles 13a and 13b of the aforementioned Directive.

The reason for the objections raised by the reviewers of the draft with regard to the repeal in Article 1 (2)(1) of the NCSA, according to which the act does not apply to telecommunications enterprises and provisions related to the amendment of the regulation in question, was fear of the destabilisation of the existing order by including telecommunications enterprises into the relatively new national cybersecurity system, which, in the opinion of the reviewers, could lead to the disruption of the existing legal order, determined both at the level of EU and Polish regulations. The regulations concerning the security of telecommunication networks and services are contained in EU

Telecommunication Directives, which have now been replaced by the European Electronic Communications Code, which is being transposed into the Polish legal order by replacing the Telecommunications Law Act with the Electronic Communications Law (draft of 29 July 2020 of the Electronic Communications Law, No. UC 45 from the list of the Government Legislation Centre). As of 30 August 2021, on the website of the Government Legislation Centre, the draft is being consulted at the EU Affairs Committee. In the opinion of the reviewers, there is no justification, both from the perspective of telecommunications enterprises and from the perspective of operators of essential services and providers of digital services, to disrupt the two systems by attempting to combine them, creating contradictory or overlapping regulations, which may moreover be contrary to European Union law. What is important is Polish telecommunications enterprises have conducted advanced works to ensure compliance with the recently adopted Regulation of the Minister of Digital Affairs of 22 June 2020 on minimum technical and organisational measures and methods, which telecommunications enterprises are required to use to ensure the security or integrity of networks or services (Regulation of the Minister of Digital Affairs of 22 June 2020 on minimum technical and organisational measures and methods, which telecommunications enterprises are required to use to ensure the security or integrity of networks or services (Journal of Laws of 2020, item 1130 of 29 June 2020)), the vacatio legis of which expired on 30 December 2020. Hence, the requirements in terms of the security of telecommunications networks and services should be the subject of the regulations contained in the proposed act, i.e., the Electronic Communications Law (ECL), and not, as initially proposed, in the National Cybersecurity System Act.

Other objections to the draft act concerned the proposed amendments, consisting in adding to Article 2 of the NCSA point 8a, which introduces a definition of the telecommunications incident understood as an incident that causes or may cause serious deterioration in the quality, or interruption of the continuity of the provision, of electronic communications services. The reviewers of the draft reported that the introduction of another type of incident (telecommunications incident) may lead to problems with the classification of incidents, while at the same time signalling that the draft does provide for the classification of any other special categories of incidents for other sectors. There were also doubts concerning the proposed Article 2(8)(g) of the Act on the National Cybersecurity System, which introduces a definition of the concept of a high-risk situation, understood as the situation referred to in Article 2 (65) of the draft act Electronic Communications Law. In the opinion of the reviewers, the aforementioned provision should only be included in the Act – Electronic Communications Law – as it defines the obligations of telecommunications enterprises. There were also doubts concerning adding to the draft of Chapter 4a addressing the obligations of electronic communication entrepreneurs, which should also be regulated within a given sector, as well as the proposal to issue in the provisions of this chapter (Article 20a (4)) the authorisation for the minister competent for computerisation, identical with the authorisation in Article 39

of the draft Act – Electronic Communications Law. A similar issue concerned Article 20c(4) of the said draft, identical to Article 42(2) of the draft Act – Electronic Communications Law. In addition, according to the reviewers of the changes proposed by the legislators, the powers of the Plenipotentiary with regard to taking over the tasks related to the handling of telecommunication incidents should also be analysed in detail.

The current position of telecommunications enterprises within the cybersecurity system results from national legislation, but the basic solutions in this area are a result of the solutions adopted under European Union law. The differences with regard to telecommunications enterprises concern both obligations related to counteracting and fighting threats to cybersecurity, as well as notifying about the occurrence thereof. By entrusting relevant tasks to the President of the Office of Electronic Communications (UKE), the possibility of transmitting information about incidents occurring in the telecommunications sector to the relevant links of the national cybersecurity system is guaranteed. The structure of the sectoral regulations in the field of telecommunications cybersecurity generally corresponds to the structure of obligations with regard to operators of essential services, provided for in the general rules on cybersecurity.

The distinctiveness of the adopted cybersecurity solutions in the electronic communications sector also has its origin in EU law (Rojszczak, 2018:200). EU solutions ensuring cybersecurity in the electronic communications sector have been shaped by the provisions of Chapter III a, added in 2009 in Framework Directive 2002/21/EC. Article 13a of the Framework Directive requires the application of appropriate technical and organisational measures in the event of a threat to the security of networks and services, ensuring a level of security proportionate to the risk involved, taking into account the state of the art. Enterprises are required to protect network integrity to ensure continuity of service provision and should notify the regulator of any breach of security or a significant loss of network integrity. The legislation provides for Member States to notify each other of these matters, as well as to inform the European Network and Information Security Agency (ENISA) of the occurrence of threats. Pursuant to Article 13b of the Framework Directive, the national regulator should have the right to issue binding instructions to enterprises on matters concerning network and service security, to request information from them and to require them to submit to a security audit at their own expense. The NIS Directive further solidified this stance; in recital seven of the Directive, the legislator excluded enterprises providing public communications networks or publicly available electronic communications services from its scope, thus emphasising the distinctness of the electronic communications sector in terms of cyber security issues. Article 1(3) of the NIS Directive stipulates that the requirements for security and incident reporting set forth in the Directive do not apply to enterprises subject to the requirements of Articles 13a and 13b of the Framework Directive 2002/21/EC. This status should also be maintained after the implementation of the European Electronic Communications Code (ECE) (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L

321/36 of 17 December 2018). By December 2020, Member States were required to implement the provisions of the EECC, which replaces the solutions introduced by Framework Directive 2002/21/EC and comprehensively regulates cybersecurity in the electronic communications sector. Article 2(42) of the EECC defines a "security incident" as an incident that has an actual adverse effect on the security of an electronic communications network or service. It was the legislators' intent that Member States should impose obligations on network and service providers to take appropriate technical and organisational measures in the event of threats. These measures should ensure a level of security proportionate to the risk involved, taking into account the state of the art. With regard to the handling of security incidents, consideration should be given to the relevant procedures, incident detection capabilities, incident reporting and notification. At the same time, national requirements in the area of cybersecurity of the electronic communications sector should not hinder access to individual domestic markets. For this reason, Article 40(1) of the EECC entrusts ENISA with tasks aimed at avoiding discrepancies in national security requirements, which may create security risks and barriers to the internal market. The provisions of Article 40 of the EECC specify the obligations of the service provider with regard to security incidents, in particular the obligation to notify competent authorities, service and network users and to make public information about the most serious incidents. A key element of the response of network and service providers' to security incidents is informing the competent national authorities of incidents which have a significant impact on the operation of networks or services. Network and service providers should be required to provide the information necessary to assess the security level of networks and services, including documented security policies, and to undergo security audits. In March 2019, the European Commission issued recommendations on the cybersecurity of 5G networks (Commission Recommendation of 26 March 2019 Cybersecurity of 5G networks, C(2019) 2335 final). In January 2020, the European Commission published a recommendation on a common set of risk mitigation measures in the area of 5G network cybersecurity (European Commission, 2020), developed with the participation of ENISA on the basis of data provided by Member States. The document referred to as "5G Toolbox" lays the groundwork for coordinated, joint action by EU countries to ensure 5G network security.

Sectoral obligations of telecommunications enterprises in the field of cybersecurity are set out in Articles 175-175e of the Telecommunications Law Act. The primary objective of telecommunications enterprises is to ensure the security and integrity of networks, services and communication transmission, as well as to protect the substance and functionality of the network and its ability to provide services. Measures preventing threats to the network, services and communications are of fundamental importance. The entity obliged to apply security measures to networks, services and communications is the provider of publicly available telecommunications services. Since service providers may provide services with the use of third party infrastructure, the provision of Article 175(1) also imposes this obligation on the operator of the public telecommunications

network in which the activity is carried out. Telecommunications enterprises are obliged to cooperate if it is required to ensure effective protection. The entrepreneur should take into account the relationship between the level of threats and the effort necessary to remove or reduce them, as well as ensure a level of security appropriate to the level of risk. Article175b (2) of the Telecommunications Law Act requires the Office of Electronic Communications to publish on the UKE website information about the occurrence of a breach of network security or integrity, or to impose on the telecommunications enterprise, by way of a decision, the obligation to make it public (indicating the manner of its publication), should it deem this to be in the public interest. Such a decision may be made immediately enforceable depending on the nature of the case. The enterprise must fulfil the information obligation at its own expense. A number of communication obligations have also been imposed on telecommunications enterprises. The President of the UKE is obliged to indicate potential threats related to telecommunications services. Telecommunications enterprises are obliged to cooperate in this regard. Since the functioning of electronic communications networks and the provision of services is of key importance for the entire cybersecurity system, telecommunications enterprises are included in the system of the notification of cybersecurity incidents. The National Cybersecurity System Act has provided, through an amendment to the Telecommunications Law Act, a mechanism for the transmission of information on cybersecurity incidents by telecommunications enterprises. Article 175a entrusts the President of the UKE with the obligation to communicate certain information received from telecommunications enterprises to the relevant Computer Security Incident Response Team (CSIRT). The sectoral mechanism of informing about cybersecurity incidents was aligned with the EU data system for such incidents. Article 175b implements in the national legal order the requirement of Article 13a(3) of the Framework Directive requiring the national regulator to inform other regulatory authorities in EU Member States and ENISA about breaches of network and service security. The separation of Chapter 7a "Security and integrity of telecommunication networks and services" in the Telecommunications Law Act and the establishment of a separate sanction regarding the fulfilment of cybersecurity obligations by telecommunications enterprises highlights the importance of these obligations for the functioning of the telecommunications sector. Provisions of Article 175c, based on relevant solutions of EU law, provides the basis for active prevention by telecommunications enterprises, under the supervision of the regulator, of threats to both the security and integrity of networks and services resulting from the transmission of communications that may pose a threat to them. The most decisive measures for counteracting threats to network security, services and communication transmission are provided for in Article 175c of the Telecommunications Law Act. Such measures lead to the termination of transmission handling or network termination that are generating threats. An incidental measure provided for in Article 175c(1)(1) consists in the elimination of communication transmission. This means that the entrepreneur, upon identifying a threat related to a particular communication, ceases its handling, in particular its transmission, processing or storage, depending on the type of telecommunication service provided. Article 175c

does not impose an obligation to inform the user about the elimination of the communication transmission, although there is no legal obstacle for the entrepreneur to do so. The second measure, of a permanent nature, provided for in Article 175c(1)(2), consists in the interruption or limitation of the provision of telecommunications service at the network termination level. This measure concerns services of a specific type or all services provided to the termination of this network. The entrepreneur is required to immediately inform the President of the UKE about the application of a measure eliminating communications and interrupting or limiting the services. In the event of a decision of the President of the UKE prohibiting the use of restrictions, the subscriber may hold the entrepreneur liable. In order to assess the status of telecommunications enterprises in the national cybersecurity system, it is important to remember that a telecommunications enterprise, due to the nature of its business, may at the same time be an operator of essential services. Operators of these services are part of the national cybersecurity system. The list of essential services contained in Annex 1 to the Act includes in the digital infrastructure sector "Entities that provide DNS services". Telecommunications enterprises use DNS servers in their business activities to provide data transmission services to their clients. The Act on the National Cybersecurity System does not define terms related to a DNS service. The relevant definitions can be found in the NIS Directive. In Article 4(14) of the NIS Directive, "domain name system (DNS)" is defined as "a hierarchical distributed network name system that responds to requests for domain names". In turn, Article 4(15) of that Directive, defines "DNS service provider" as "the entity that provides DNS services over the ". The problem concerning the application of the provisions on DNS service provision to telecommunications enterprises arose at the stage drafting the NCSA and later in connection with the preparation of the regulation provided for in Article 6 of the NCSA. As part of the work on the draft act, the Council for Digital Affairs indicated in its comments that "an entity providing DNS services is almost every provider making its systems available to customers and every cafe providing its customers with free access". With regard to that, the Minister of Digital Affairs explained that "the identification of a given entity as an operator of essential services will also depend on the thresholds established under Article 6" (Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and on significance thresholds for the consequences of incidents disrupting the provision of essential services, Journal of Laws of 2018, item 1806 of 21 September 2018). The problem emerged again during the work on the regulation setting these thresholds. During these works, it was noted that a great number of -access service providers also provide their customers with functions based on their own DNS servers as part of these services. Chambers of commerce operating in telecommunications noted that DNS services were in practice provided by telecommunications enterprises, and that the service itself was an integral part of, or accompanied the provision of, telecommunications services.

In this regard, it was postulated that due to the scope and comprehensive nature of cybersecurity obligations provided for in Telecommunications Law Act, the exemption from the act should also apply to telecommunications enterprises also, if these provide authoritative DNS server services. This postulate was rejected by the Minister of Digital Affairs, who explained that the statutory exemption applied to telecommunications enterprises to the extent to which they were covered by the Telecommunications Law Act. In turn, entities providing DNS services may be considered as operators of essential services regardless of whether they are telecommunications enterprises or not. This issue was also considered at the EU level in connection with the adoption of the NIS Directive. Annex I of the Commission Communication "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union" (COM(2017) 476 final ANNEX 1) clarifies in section 5.2 the case of telecommunications enterprises carrying out activity in the field of DNS. The Communication states that the security and incident reporting requirements of the Directive do not apply to providers that are subject to the requirements of Articles 13a and 13b of the Framework Directive 2002/21/EC, namely entrepreneurs providing public communications networks or publicly available electronic communications services. If, however, such an entrepreneur also happens to provide DNS services, then it will be subject to the security and incident reporting requirements of the NIS Directive. Member States are required to conduct an identification process in accordance with Article 5(2) of the NIS Directive and identify those individual DNS providers who should be subject to the requirements of the NIS Directive due to the fulfilment of the criteria set out in Article 5(2) of that Directive. In view of the above, telecommunications enterprises are not automatically excluded from the scope of the NIS Directive and, consequently, from the scope of the National Cybersecurity System Act if they provide DNS services within the scope indicated in the NIS Directive and national legislation. For this reason, in each case, it is necessary to assess whether an entrepreneur is an "entity that provides DNS services" within the meaning of the NCSA, taking into account the meanings given to the individual terms in the NIS Directive. It follows from the above-mentioned national and EU legal acts that DNS infrastructure may be used as part of the activities conducted by the telecommunications entrepreneur, as an integral part of telecommunications service (electronic communications service). The use of DNS servers by a telecommunications entrepreneur as part of its own activity consisting in the provision of telecommunications services does not constitute the provision of DNS services. Information on security breaches of telecommunication services and networks, which constitute incidents with respect to DNS infrastructure operated by a telecommunications enterprise, is communicated to the President of the UKE, who sends it to the relevant CSIRT on the terms specified in the Telecommunications Law Act. However, the telecommunications enterprise may, in addition to its core business consisting in the provision of networks and telecommunications services, also provide DNS services separately. In such a case, the telecommunications enterprise is also a DNS service provider. It follows from the Directive that the provision of DNS services should be independent of the provision of

telecommunications services. In light of the provisions of the NCSA and the NIS Directive, there may be a situation in which an enterprise is both a telecommunications entrepreneur and a DNS service provider. However, such an entity does not become a DNS service provider due to the fact that it provides its subscribers with DNS services using its own infrastructure as part of its telecommunications business. Consequently, the reference to an "entity providing DNS services" in Annex 1 to the NCSA does not apply to telecommunications enterprises that provide DNS services only to their subscribers. The assessment regarding the application of the provisions of the NCSA to the provision of DNS services must also take into account the provisions of the Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and significant thresholds of the consequences of incidents disrupting the provision of essential services (Journal of Laws of 2018, item 1806). With regard to entities that provide DNS services, the regulation defines an essential service as "operating an authoritative DNS server" and the significance thresholds for the consequences of incidents disrupting the provision of essential services as "a minimum of 100,000 domain names for which the server is authoritative". Operating an authoritative server concerns a domain in an area over which the server in question exercises management, and responds to queries coming directly from the server's database. The response provided by such a server indicates that it was obtained from the server performing direct authentication of the name sought. Pursuant to Article 5 of the NCSA and the Regulation on the thresholds, the authority competent for cybersecurity will issue decisions on the classification of a specific entity as an operator of essential services. Ultimately, therefore, the classification of a particular entity into the category of DNS service providers will be determined by an administrative decision. In view of the above-mentioned provisions, it must be concluded that if a telecommunications entrepreneur, in addition to providing DNS functions to its subscribers, provides DNS services on the that meet the requirements specified by the regulation (authoritative nature of DNS information) and exceeds the threshold specified by the regulation (at least 100,000 domains), then such activity should be considered as providing essential services, and the telecommunications entrepreneur providing such a service will be subject to the provisions of the Telecommunications Law Act, regardless of the fact that the provisions of Articles 175-175e of the Telecommunications Law Act will apply to its activity involving the provision of telecommunications services (Besiekierska, 2019: art. 1 Nb.11). This is confirmed by the position of the Ministry of Digital Affairs, which states that if a telecommunications enterprise is recognised as an operator of essential services in the digital infrastructure sector, then it will be subject to the regulations of the NCSA. By being recognised as an operator of essential services within the meaning of the NCSA, a telecommunications enterprise has all the obligations provided for in the NCSA (including with regard to security and incident reporting requirements with respect to the essential services provided). There is good reason to reaffirm the view expressed in the literature that the NIS Directive was not intended to specify in detail the rules on electronic communications networks and services, but to extend cybersecurity regulations to a group of other entities that are of significance in

terms of the services provided or the infrastructure owned (Rojszczak, 2018:206). In practice, these entities may simultaneously provide telecommunications networks and services.

The fact that it is an actual problem is reflected by the judgments of administrative courts (VI SA/Wa 1436/19 of 11 December 2019 – Judgment of the Provincial Administrative Court in Warsaw, LEX No. 2976744). Judgment on a complaint against the decision of the Minister of Digital Affairs concerning the recognition of entities as operators of essential services (the party concerned argued that it had the status of a telecommunications entrepreneur and, therefore, Article 1(2)(1) of the Act of 5 July 2018 on the National Cybersecurity System applied to it, in accordance with which the act in question does not apply to telecommunications entrepreneurs in terms of security and incident reporting requirements). The Minister of Digital Affairs issued a decision recognising the Party as an operator of essential services, explaining in its rationale that the traffic exchange point service, which was the subject of the proceedings, could not be classified as a telecommunications service as defined in Article 2(48) of the Telecommunications Law Act. Therefore, to the extent in which the Party provided the aforementioned service (traffic exchange point), it could not enjoy exemption from the application of the NCSA as introduced by Article 1 (2)(1) thereof. In the opinion of the said authority, the criteria for recognising the entity as an operator of essential services provided for in Article 5(2) of the NCSA were fulfilled – the Party provided essential services which relied on information systems, and an incident would have had a significant disruptive effect on the provision thereof. In addition, when deciding on an interpretation, the court assumed that the information provided by the party that it currently operates an traffic exchange point supporting at least 100 autonomous systems was sufficient to consider the entity as an operator of essential services.

Subsequently, the party accepted the position of the court as regards the possibility to consider a telecommunications enterprise as the operator of essential services, while questioning the legal classification of the traffic exchange point service adopted by the authority. According to the Party, this service falls within the concept of a telecommunications service, as defined in Article 2(48). According to the definition, a telecommunications service is a service consisting mainly in the transmission of signals in a telecommunications network. The authority did not share this view and opined that traffic exchange at an exchange point (IXP) took place in the transport layer of the OSI network model (layer 4), while the telecommunications service, as defined in Article 2(48) of the Telecommunications Law Act, was provided at the physical layer (layer 1) thereof, being valid reason to conclude that the IXP service does not have the features of a telecommunications service. According to the Minister of Digital Affairs, there was no doubt that the IXP service required the existence of a telecommunications service (i.e., a physical layer) in order to be implemented, but it was not identical to this service. Similarly, the provision of financial advice over the phone does not become a telecommunications service simply by reason of relying on a specific communication

tool. The legislators stated that: "a telecommunications service consists mainly in the transmission of signals in a telecommunications network". Such a definition places emphasis on the fact that the telecommunications service in fundamentally about the transmission of signals, and not about the transmission of signals in addition to other aspects. Therefore, if signal transmission is only the background aspect of the service, the essence of which is to facilitate the exchange of traffic generated by different providers, it does not affect the classification of this service as not falling within the definition of a telecommunications service, as defined in Article 2(48) of the Telecommunications Law Act. The exemption from the application of the provisions of the NCSA regarding the security and incident reporting requirements applies to telecommunications enterprises, albeit extending only to activities that are specific to a telecommunications enterprise as defined in Article 2(27). Pursuant to the said regulation, a telecommunications enterprise is an entrepreneur or another entity authorised to conduct business activities under separate regulations, consisting in the provision of telecommunications networks and the provision of accompanying services or telecommunications services. Since the traffic exchange point service does not fall within any of the categories of activity of a telecommunications enterprise listed in this provision (for the reasons mentioned above), a telecommunications entrepreneur that provides such IXP services is not subject to the provisions of Article 1(2)(1) of the NCSA. In other words, as indicated in the rationale for the Decision, the obligations under the NCSA apply in their entirety to a telecommunications enterprise that operates an traffic exchange point and has been recognised as an operator of essential services. Therefore, if the telecommunications enterprise engages only in the activities listed in Article 2(27) of the Telecommunications Law Act, it may enjoy the exemption provided for in Article 1 (2)(1) of the NCSA and is not subject to the provisions of this act with regard to security and incident reporting requirements.

Therefore, regardless of whether or not an traffic exchange point service is a telecommunications service, it is subject to the legal regime establishing the national cybersecurity system (it was listed in the Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and significance thresholds for the consequences of incidents disrupting the provision of essential services), and the provisions establishing this system, i.e. the National Cybersecurity System Act (NCSA) and implementing regulations, have the nature of special provisions in relation to the Telecommunications Law Act.

Regarding the doubts concerning the scope of the obligations of a telecommunications entrepreneur that has been recognised as an operator of essential services, the superior authority has decided that since a telecommunications entrepreneur has been recognised as an operator of essential services in view of its providing a service that does not fall within the activities of a telecommunications enterprise, the exemption referred to in Article 1(2)(1) of the NCSA does not apply to it. In such a case, the fact of having the

status of a telecommunications enterprise is irrelevant. The authority's opinion was shared by the Provincial Administrative Court in Warsaw, which stated in its rationale that the dispute in this case concerned, in fact, the interpretation of the provisions of the Act of 5 July 2018 on the National Cybersecurity System and their relationship with the provisions of the Telecommunications Law Act. In the court's opinion, the Minister of Digital Affairs, in the course of administrative proceedings, correctly interpreted the law and rightfully recognised the party in the proceedings as an operator of essential services consisting in operating an traffic exchange point (IXP). The court emphasised that the interpretation adopted by the superior authority, contrary to the claim of the complainant, did not mean that the exemption provided for in Article 1(2)(1) of the NCSA was in practice ineffective and illegitimate. It applies to telecommunications entrepreneurs with regard to their activities listed in Article 2 (27) of the Telecommunications Law Act. Notably, the National Cybersecurity System Act and its implementing regulations are special provisions in relation to the Telecommunications Law Act. The court fully supported the position of the superior authority that a party providing an traffic exchange point service of a certain size must be considered an operator of essential services within the meaning of the National Cybersecurity System Act.

The above-discussed example of discrepancies in the practical interpretation of the applicable provisions could undoubtedly prompt the legislators to amend the draft act amending the National Cybersecurity System Act. However, in the light of the arguments cited here regarding the interpretation of the entirety of regulations governing the responsibility of telecommunications entrepreneurs with regard to tasks related to cybersecurity, the accusations against the Minister of Digital Affairs, as the initiator of changes to the National Cybersecurity System Act, should be considered valid.

Ultimately, the subjective scope and, by extension, the title of the draft act was changed (the draft of 20 January 2021, entitled "Act on amending the National Cybersecurity System Act and the Telecommunications Law Act" – as of 30 August 2021), and the legislators added electronic communication entrepreneurs to the objective scope of the National Cybersecurity System Act, only with respect to their obligation to comply with the requirements set out in Chapter 11b concerning the creation of a strategic communication network and the appointment of a strategic communication network operator in order to ensure the performance of tasks related to defence, state security, public security and order in the field of telecommunications. The requirements of Articles 66a-66c concerning conducting proceedings, issuing decisions and further handling of products and services provided by a high-risk provider, Articles 67a-67b concerning the tasks and powers of a plenipotentiary related to the occurrence of a critical incident, and Articles 73-74 concerning penalties imposed by way of a decision by the authority competent for cybersecurity. In addition, in order to ensure consistency of the legal system, the reference to the definitions of an electronic communication entrepreneur, the provision of a telecommunications network, electronic communication services,

telecommunications terminal devices and special risk situations contained in the Act – Electronic Communication Law were left in the amendment of the act.

References:

Besiekierska, A. (ed.) (2019) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warszawa: Wydawnictwo C.H. Beck), art.1, Nb.11.

European Commission (2020) C*ybersecurity of 5G networks EU Toolbox of risk mitigating measures*, available at: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5gnetworks-eu-toolbox-risk-mitigating-measures (August 25, 2021).

Najwyższa Izba Kontroli (2019) *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego* (Warszawa 2019), available at: https://www.nik.gov.pl/kontrole/P/18/006/ (August 30, 2021).

Rojszczak, M. (2018) Cyberbezpieczeństwo w łączności elektronicznej, In: Banasiński, C. (ed.) *Cyberbezpieczeństwo* (Warszawa: Wolters Kluwer), p. 200.

Personal Data Serving the Purpose of Ensuring State Security. Cyberspace Challenges. The European Context

JUSTYNA KUREK

Abstract Information of a personal character constitutes a special category of data used by the state and its bodies in the performance of public tasks. Difficulties in identifying risks and challenges are connected, inter alia, with the fact that the material scope of the definition of personal data is not a standing concept. It cannot be determined in advance whether a given category of information will be of a personal character or not. These risks are further aggravated when Big Data tools are used, which facilitate the effective analysis of huge volumes of data, linking information with different sources of origin, and the indirect identification of data subjects. In addition to the problems resulting from the nature of personal data, there is a further complicated problem resulting from the hybrid nature of legal regulations. This is due to the fact that some processes involving personal data processing are within the Community regime of personal data protection, while some others, as activities implemented as national security tasks, are excluded completely from the European regime. The purpose of this article is to identify the threats and problems in these conditions and the related implications for state security.

Keywords: • personal data • state security • cyberspace • Big Data • PESEL

CORRESPONDENCE ADDRESS: Justyna Kurek, Ph.D., dr. habil., Associate Professor, War Studies University in Warsaw, Faculty of National Security, State Security Institute, Political Security Department, Aleja Generala Antoniego Chrusciela "Montera" 103, 00-910 Warszawa, Poland, e-mail: j.kurek@akademia.mil.pl, ORCID: 0000-0002-8754-5243.

https://doi.org/10.4335/2022.2.8 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introductory remarks

Information of a personal character constitutes a special category of data used by the state and its bodies in the performance of public tasks. They often constitute the building blocks of public services. Without this type of data, it would be impossible to conduct public or economic activities (Karpiuk 2015:13). Difficulties in identifying threats and challenges in this area are related to the fact that the material scope of the definition of personal data is not a standing concept. It is significantly affected by the development of information techniques and technologies. As noted in literature, based on the reference to the criterion of "technological progress", it can be simultaneously stated that the scope of the term "personal data" may change over time, because the information that we are currently unable to link to a specific person, in the perspective of progressive civilisation and technological development, may be qualified in this manner in the future (Fisher, Górski, Nerka, Sakowska-Baryła, Wygoda, 2018:71-72). Thus, depending on the technical and technological identification possibilities, personal data can be, among other things, photographs, videos, biometric data, facial features or fingerprints. The danger for the state and its undisturbed functioning is further implied by the fact that the concept of personal data is extremely capacious. It cannot be determined in advance whether a given category of information will be of a personal character or not. These risks are further aggravated when Big data tools are used, which facilitate the effective analysis of huge volumes of data, the linking of information with different sources of origin and the indirect identification of data subjects. In addition to the problems resulting from the nature of personal data, there is a further complicated problem resulting from the hybrid nature of legal regulations. This is due to the fact that some processes involving personal data processing are within the Community regime of personal data protection, while some others, as activities implemented as national security tasks, are excluded completely from the European regime. The purpose of this article is to identify the threats and problems for personal data processing and the related implications for security.

2 The concept of personal data

Pursuant to Article 4(1) of the GDPR, personal data mean any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The definition adopted in the GDPR is horizontal in nature and applies in whole to the protection of personal data under European Union law. The source literature notes the fact that any information, regardless of the manner and form in which it is expressed, and no matter if it is widely understood, can be regarded as personal data. The legal nature of any such information should be assessed individually for each of its holders (Sibiga, 2003:33). It is not possible to exclude in advance any category of information from the scope of personal data.

Under the GDPR, there is no doubt that the term "personal data" should be construed as individual information about personal and factual relations of a specified or specifiable natural person. The concept of personal data does not cover information of an anonymous character, which makes it impossible to identify natural persons beyond reasonable doubt; as well as entities other than natural persons. On the one hand, the attribution of the quality of personal data to a given piece of information will, therefore, depend on external factors and the technological possibilities to identify that person. It is not essential that the data subject is known to the data processor. The legislation only requires that it should be specified (Däubler, Hjort, Schubert, Wolmerath 2010: § 3 BDSG *[Federal Data Protection Act]*). Identification, on the other hand, means that a person can be distinguished within a group from other group members. This, however, does not have to mean that the person is identified by their first and last name. It is sufficient to indicate circumstances which make it possible to identify this person uniquely (Drozd, 2008:24). It is also assumed that a person is identifiable, if – although not yet identified – such identification is possible. The source literature notes the fact that any information, regardless of the manner and form in which it is expressed, and no matter if it is widely understood, can be regarded as personal data. The legal nature of any such information should be assessed individually for each of its holders (Sibiga, 2003: 33). Therefore, from the point of view of implementing public tasks in the area of security, all information with identifiable potential must be subjected to special protection.

3 The impact of Big Data analytics on state security with regard to personal data

Big Data processes have caused a revolution in the analysis and processing of personal data, increasing the potential for their use. Technological developments mean that the character of personal data can be attributed to broad categories of information. The new analytical potential, apart from the broader benefits, also implies obligations, in particular towards personal data subjects. Since it is difficult to exclude *a priori* the personal character of various pieces of information, the protection of personal data should be extended to various categories of information held by the data subject in case this information, through the way it is linked to other information, acquires a personal character. The potential of Big Data further increases the analytical possibilities. The value of data can be increased not only through new processes of acquisition and analysis, but thanks to linking certain data with data from other sources. Often, the mere synthesis of unclassified data from, for example, public registers and social networks, owing to the use of analytical tools with strong data structuring capabilities, typical of Big Data analytics, can be threatening from the point of view of state security.

4 The hybrid nature of personal data regulations – the European context

One of the most interesting challenges for the state in the era of big data analytics is the issue of personal data protection and the use of personal information under the conditions of mass processing. From the point of view of state security, ensuring the protection of personal data is additionally connected with the necessity to function in a complex legal regime, which is created by intermingling national and EU regulations. The framework for the protection of personal data, established in the Treaty, plays a key role in structuring a personal data protection system. Pursuant to Article 72, in connection with Article 73, of the Treaty on the Functioning of the European Union, the legislative competence of the European Union shall be excluded in the case of activities which lie outside the scope of the Union law, in particular those relating to national security. This distinction is of particular importance in the area of personal data protection. Indeed, EU law on the protection of personal data is excluded for the regulatory areas which are not subject to European Union law (Article 16(2) of the TFEU). The regulatory framework adopted at a European Union level in the area of personal data protection consists of three instruments: (1) the General Data Protection Regulation (GDPR), (2) Directive (EU) 2016/680 (known as the Police Directive), and (3) Regulation (EU) 2018/1725 concerning the processing of personal data by EU bodies. The exclusion, under the GDPR and Directive 2016/680/EU, of the processing of personal data in the course of activities that fall outside the scope of Union law, including in particular activities within the scope of national security and the activities of entities carrying out tasks in the area of national security, leads, in effect, to a kind of regulatory regime of a hybrid nature – since some processes involving personal data processing are covered by Union law and some others are up to the arbitrary decision of the national legislator. The indicated regulatory context and the attempt at providing a systemic inclusion of the legal framework for personal data protection prompt a proposal for the adoption of the paradigm of a hybrid legal regulation (Kurek, 2021:18-19). A hybrid legal environment has already been *per se* a source of risk for security. This is because neither the Treaty provisions, nor the data protection provisions, define what national security is.

5 Personal data in land and mortgage registers from the perspective of state security

Data from land and mortgage registers may serve as an example. Such registers, apart from information relating strictly to real property, also contain information about owners as well as data on the financing of the property in the form of credit and mortgages encumbering the property. Although safeguards against unauthorised access are introduced in the explicit version of the interface, they are not of an absolute nature. The "anti-bot" mechanism does not require any intellectual effort, but only the ticking of the appropriate box. Also, limiting the search options to one criterion – the number of the land and mortgage register – does not protect the system. The designation of court districts is pre-definable, the numbers of registers are not assigned on a random basis, and the

control number is a combination of ten variations. Hence, this data can be obtained by suitably programmed robots and placed in a relationally structured database. By linking these data with information from social networks, it is possible to accurately determine the family circles of the property owner. Additionally, social networks contain photos and information about users' "check-ins". Unauthorised access to such information alone poses a threat not only to the privacy of data subjects, but also to the security of persons and property (Kurek 2021:136 ff).

6 The delivery of personal data from the PESEL database to Polish Post – a case study

From the point of view of state security, an extremely interesting case study arises from a project that was not implemented, which assumed the use of the PESEL database by Polish Post (Poczta Polska) for the purposes of organising the presidential elections by post. The objective of the following analysis is not to assess the correctness of the organisation of the presidential elections or lack thereof, but only to examine whether adequate precautions were taken with regards to personal data, and to indicate the risks which could arise for state security from any possible irregularities in data security.

PESEL (Universal Electronic System for Registration of the Population) is one of the basic registers in Poland. It contains information about Polish citizens and foreigners who have a PESEL number. This database operates on the basis of the provisions of the Act of 24 September 2010 on the Population Register. Thus, the PESEL register contains information making it possible to determine the status of a natural person. The provisions of the Act on the Population Register also define who may enter data into the PESEL database. However, they do not regulate the scope of entities with access to the system. According to information provided on the website of the Ministry of Digitalisation, the data can be accessed via secure connections by enumerated entities, including but not limited to election authorities, such as: public administration authorities, courts, state and local government organisational units.

Therefore, the public PESEL register contains contact details essential from the point of view of the potential organisation of postal voting, but under the law only those regarding a permanent place of registered residence or a voluntarily declared place of temporary residence. A list of electors is drawn up based on data from the PESEL register, but in accordance with adopted legal regulations, the list is verified on the basis of voluntarily declared places of residence by persons wishing to be added to the list of electors.

Under the anti-crisis shield, permission was granted (under the provisions of the Act of 16 April 2020 on Specific Support Instruments in connection with the Spread of the SARS-CoV-2 Virus) to provide the postal operator with the data from the PESEL register for the purposes of organising the elections. Pursuant to Article 99 of the afore-said Act, the designated operator, after submitting a request in electronic form, shall receive data

from the PESEL register or from other listings or registers being at the disposal of a public administration body, if the data are needed to perform tasks related to the organisation of the election of the President of the Republic of Poland or in order to perform other duties imposed by government administration bodies. On 22 April, Polish Post received data from the PESEL system exported on a DVD. The data were delivered on an encrypted carrier by convoy. Therefore, the delivery was contrary to statutory disposition, where it is indicated that access shall be provided in electronic form. Pursuant to Article 78^2 § 1 of the Civil Code, for the observance of the written form of an act in law, it is sufficient to make a declaration of intent and append a qualified electronic signature thereto. Delivery by convoy together with a password, which is sent through a different channel, does not meet the requirements of a qualified electronic signature. The explanations in no way indicate that the disc was secured with a qualified electronic signature. The fact of providing the password via other channels confirms the assumption that the data was secured outside the key public infrastructure. This situation seems completely incomprehensible in the light of the explanations of the Ministry of Digitalisation to the Ombudsman, according to which, at the time of delivery of the data Polish Post, by virtue of the Decision of the Minister of Internal Affairs of 8 September 2014 No. DSO-WUI-6173-24.2/14, had access to the PESEL register by means of devices for remote transmission of data for the performance of statutory tasks (https://www.rpo.gov.pl/sites/default/files/Odpowied%C5%BA%20MC%20%20dane%20przekazane%20Poczcie%2C%204.05.pdf). It is not entirely clear why the access already held could not be used.

The transmission of exported data to the disc implies the assumption that personal data from the PESEL register were, or were supposed to be, processed outside a secure environment. It is worth pointing out that other entities using the PESEL database may use it only at isolated workstations within a secure dedicated network. The condition is such that workstations are not allowed to have access to the internet.

Generating and storing data on a data carrier was, therefore, unnecessary and only posed a risk for personal information. According to the explanations of the Minister of Digitisation, the reason for data delivery on a disc in a structured form resulted from the fact that the interface of the system used by the designated operator did not enable the mass downloading of data and the preparation for sending election packages. From an IT point of view, it may have been sufficient for the data controller to change user rights and access levels.

In accordance with the declaration of the Minister of Digitisation, the delivered disc contained only indispensable data – that is the data of living Polish citizens who had reached legal age by 10 May 2020 and whose country of residence was Poland. The provided data included: PESEL numbers, first name(s), surnames and, depending on what data the person had registered in the PESEL register, their current address of permanent residence, and if there was no such address, the last address of permanent residence and

an address of temporary residence. Additional information provided gave notice of whether a person had currently registered a temporary trip outside the country (without specifying the country of departure).

From the point of view of the legal regulations on the protection of personal data, in particular in the light of Article 14 of the GDPR, the delivery could be considered admissible if it followed from the law that the data were provided for the purpose of the implementation of a task regulated by an act. The provision of Article 99, in the absence of an act on postal elections, does not seem sufficient in view of the disposition of Article 14 of the GDPR. The second element, which is important from the point of view of the legal regulations on the protection of personal data, is carrying out, at the stage of drafting a legal act, the proper analysis of the impact of the processing of personal data. The grounds for the governmental draft act (Parliamentary Paper no. 330) do not refer at all to the provision of data from the PESEL database. Significantly, as regards personal data and the impact of the regulation on personal data, the grounds refer only to the context of obtaining data on the financial situations of entrepreneurs applying for support in the light of Article 10a of the said Act, indicating that the principles regarding the protection of personal data shall not apply to the regulation (http://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=330). Neither the delivery of the PESEL database nor Article 99 are grounded. In this situation, it cannot be stated that any analysis of the impact of the regulation on personal data protection was made at the stage of drafting the legal act.

Thus, in the light of the disposition of Article 25 of the GDPR, neither the Ministry of Digitisation, nor Polish Post could abstain from carrying out an analysis of the impact of the processing of personal data under a risk-based approach. Also, due to the lack of an analysis, in the light of Article 14 of the GDPR, there were no grounds for abandoning the obligation to provide information to data subjects. The analysis would have demonstrated the existence of risks at multiple levels, not only to data subjects but also to state security.

The risk for security had already emerged at the stage of exporting the data to a DVD carrier and encrypting it. Securing the delivery with a qualified electronic signature within the meaning of Regulation 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market relies on a key public infrastructure using asymmetric encryption. This guarantees that any subsequent changes to the electronic data or interference is immediately noticeable by the recipient of the delivery. In the conditions of password-protected data delivery, there is no such effect.

Secondly, the delivery of data outside a secure IT environment exposes it to additional risks of a physical nature. A hostile takeover of a convoy could result in the structured data of both Poles and foreigners registered in the PESEL database being out of control

and could be used contrary to its purpose. On the other hand, multiplication of the database would be beyond any control.

The creation of a parallel database could make it possible to generate dummy identity documents and steal the identity of millions of people. Information such as first names, last names, PESEL numbers and permanent addresses are data used for authentication in the case of many services, including public services. The extraction of such data makes it possible, with the additional extraction of data from publicly available sources, to steal identities. They could be used to extort credit via the internet, to obtain fast loans where identification is simplified, and to conclude telecommunications contracts on behalf of the data subject, and this could lead to many other activities destabilising economic circulation and national security.

Even if the delivery and convoy itself do not cause problems, the provision of data outside a secure remote transmission also means that data retrieval is not controlled. According to the procedures applicable to the PESEL database, entities authorised to access the database may use the information only for the purpose of performing their duties. Access is obtained by means of remote transmission, through devices allowing the identification of the person obtaining data in the system and the scope, date and purpose of obtaining it. These entities must have technical and organisational safeguards making it impossible to use such data not in accordance with the purpose for which they were obtained (Czaplicki, 2015:144). With regard to standard queries to the PESEL database, each query by an authorised entity involves the identification of the entity through secure devices. The acquisition of data by an employee of a certain institution, which was not authorised by public tasks, was also easy to determine. This procedure gave a sense of control over the system. This made it possible in the past to control and detect unusual traffic in two bailiff offices, where 350,000 records were retrieved from the PESEL database inconsistently with the scope of tasks (https://www.money.pl/gospodarka/wiadomosci/artykul/pesel-dane-komornik-wyciek,237,0,2393581.html).

The delivery of data outside of a remote transmission is an exception and, unfortunately, it does not secure them against unauthorised access. Data from the DVD, in the possession of Polish Post, may be used beyond access control and entered into the system outside of a secure environment, thus generating numerous risks for state security, including the security of the Polish legal system and economic circulation.

The process of providing the data generated a risk not only for the security of the persons whose data are included in the public register, but also for the security of the state. The way in which the personal data were to be used in the elections should also raise serious doubts. Direct delivery of election packages to boxes at permanent addresses could not ensure data security nor the security of the election process itself. There is certainly a very large group of people who do not live at their permanent addresses. These people add

themselves to the list of electors in their place of residence. In addition, the obligation to inform authorities about changing a place of residence for more than three months is often not respected. Therefore, the proposed voting model assumed no control over who actually casts a vote, which, from the point of view of political security, undermines the credibility of potential results. It would result in a lack of democratic legitimacy for the body so established. A permanent address may be inhabited by completely different people than those who are registered there. Furthermore, Polish Post had no possibility to identify the declarations, which were to be submitted together with the votes, stating that they were cast by themselves. It does not have access to specimen signatures.

It is also worth paying attention to the physical risk of putting documents containing personal data into postboxes. Postboxes in blocks of flats and on housing estates do not have any special protection. They are often an element of public space. Therefore, the possibility of getting into them is very easy.

Looking at the risks indicated above, it should be stated that neither Polish Post, nor the provisions of the Act that created the framework for the delivery of information in any systemic way, guaranteed that any personal data protection standards were maintained. On the contrary, they generated serious risks for personal data. In addition, the legal regulations did not contain any mechanisms for the erasure of data no longer necessary for the purpose for which they were obtained. Despite the fact that the general election by postal ballot has not taken place, there is no documentation whatsoever confirming the erasure of data, the destruction of carriers, or data anonymisation. Under these circumstances, the Minister of Digitalisation should not have provided data to the postal operator from the beginning of the process, as this process did not guarantee any level of security for personal data.

7 Conclusions

Information of a personal character constitutes a special category of data used by the state and its bodies in the performance of their tasks in the area of security. Much of this information will correspond to a flexible definition of personal data. As indicated by the considerations made hereinabove, the scope of the term “personal data” may change over time, because the information that we are currently unable to link to a specific person, in the perspective of the progressive development of civilisation and technology may be qualified in this manner in the future (Fisher, Górski, Nerka, Sakowska-Baryła, Wygoda, 2018:72). Entities performing tasks in the area of security also take part in the processing of information of a personal character. For these entities, the challenges are double. Thus, the challenge faced by entities performing tasks in the area of security is to protect essential national values, at the same time maintaining the protection of citizens’ privacy and dignity. Thus, a particular challenge is to ensure a balance between the effective counteraction of threats to state security and the protection of citizens’ privacy. The problem of state security in connection with the processing of personal data is

accompanied by the problem of the hybrid nature of legal regulations. From the point of view of state security, ensuring personal data protection is additionally connected with the necessity to function in a complex legal regime, which is created by intermingling national and EU regulations. The indicated regulatory context and the attempt at a systemic inclusion of a legal framework for personal data protection prompts a proposal for the adoption of the paradigm of a hybrid legal regulation (Kurek, 2021:18-19), which *per se* constitutes a source of risk for state security resulting, for example, from the lack of a precise definition of the term "national security".

References:

Czaplicki, P. (2015) Identyfikacja tożsamości użytkowników publicznych baz danych, In: Szpor, G. (ed.) *Internet. Publiczne bazy danych i Big Data* (Warsaw: C.H. Beck), pp. 137-147.

Däubler, W., Hjort, J.P., Schubert, M. & Wolmerath, M. (2010) *Arbeitsrecht, Komentarz* (Baden-Baden: C.H. Beck).

Drozd, A. (2008) Pojęcie danych osobowych, In: Fajgielski, P. (ed.) *Ochrona danych osobowych z perspektywy dziesięciolecia* (Lublin: Wydawnictwo Katolickiego Uniwersytetu Lubelskiego), pp. 1-202.

Fisher, B., Górski, M., Nerka, A., Sakowska-Baryła, M. & Wygoda, K. (2018), In: Sakowska-Baryła, M. (ed.) *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz* (Warszawa: C.H. Beck), pp. 1-652.

Karpiuk, M. & Chałubińska-Jentkiewicz, K. (2015) *Prawo bezpieczeństwa informacyjnego* (Warszawa: Wydawnictwo Akademii Obrony Narodowej).

Kurek, J. (2021) *Bezpieczeństwo państwa w warunkach hybridowej regulacji danych osobowych w dobie analizy Big data. Aspekty prawne, organizacyjne i systemowe* (Warszawa: Wydawnictwo Akademii Sztuki Wojennej), pp. 1-319.

Sibiga, G. (2003) *Postępowanie w sprawie ochrony danych osobowych* (Warszawa: Dom Wydawniczy ABC), pp. 1-228.

Cybersecurity of Drone Operations in Public Space

TADEUSZ ZIELIŃSKI

Abstract Drones, have been the focus of business, military and public attention for several decades, showing potential in both civilian and military applications. The use of drones in the public domain may pose certain risks related to the safety of citizens and their property Particularly significant are the risks associated with taking control of the UAVs or the theft of data collected by drones through cyberattacks targeted at individual system components. The issue of ensuring the security of drone operations in public spaces requires a comprehensive approach. In this respect, it will be necessary to strengthen the cooperation between producers of UAV components, state administration authorities and services responsible for broadly defined security and public order.

Keywords: • cybersecurity • cyberattack • cyberthreat • drone • UAV • public space

CORRESPONDENCE ADDRESS: Tadeusz Zieliński, Ph.D., Associate Professor, War Studies University in Warsaw, Military Faculty, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: t-zielinski@akademia.mil.pl, ORCID 0000-0003-0605-7684, Researcher ID V-6001-2018.

https://doi.org/10.4335/2022.2.9 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Unmanned aerial vehicles (UAVs), commonly referred to as drones, have been the focus of business, military and public attention for several decades. They show potential in both civilian and military applications. Despite the fact that this technology was originally designed for the military – as yet another tool to be utilised in armed conflicts, offering an advantage over potential adversaries – it was very quickly adapted to civilian needs. Nowadays, drones can be regarded as "dual-use" technology.

It should be stressed that drones are used more and more extensively for civilian purposes. This is due to the emergence of new, transformative technologies that expand the capabilities offered by UAVs. In turn, more and more flexible legal regulations introduced at various levels, including global (i.e., the International Civil Aviation Organization, ICAO), regional (i.e., the European Aviation Safety Agency, EASA) and national, are making drones available to a wide range of users who often use them in innovative ways. As a consequence, drones increasingly appear not only in dedicated airspace but also in the public domain. This trend will grow and in the future, drones can be expected to be used in cities as aerial, automated or autonomous taxis, completing various deliveries or supporting certain law enforcement services. One can imagine that they will operate in airspace under similar rules as those applicable to other airspace users, performing various operations without exciting much interest from other users.

However, it should be remembered that UAVs are not capable of carrying out tasks entirely independently. Rather, they are part of a system composed, *inter alia*, of a control station, an operator, a communication link, and sensors – all of which enable UAV operations. Without these elements, drones cannot function properly and the safe performance of their operations is affected by the overall incidence of undesirable phenomena compromising the safety of individual system components. Particularly significant are the risks associated with taking control of the UAVs or the theft of data collected by drones through cyberattacks targeted at individual system components. It is easy to imagine the danger posed by terrorist or criminal groups taking unauthorised control of a drone to deploy it in public spaces, e.g., during a mass event or in a crowded city centre.

2 The potential use of drones for civilian purposes – examples

It is virtually impossible to list all the potential uses of drones for civilian purposes. The scope of their use is likely limited merely by human imagination, legal regulations and technological constraints. Nevertheless, the use of drones for civilian purposes can be divided into three main fields: a) support of services responsible for ensuring broadly defined security and public order; b) crisis management; and c) commercial use. It should be emphasised that this is not a closed list, but only some of the numerous potential use options. In addition, the use of drones will also depend on their capabilities and constraints resulting from the class they represent. Class I includes UAVs with a take-off

weight of less than 150 kg, which can be further divided into micro, mini and small UAVs. This class does not require any certification standards. Such drones are generally equipped with mixed sensors (optoelectronic and infrared) and are characterised by relatively low logistic requirements. They operate at low altitudes not exceeding 1,600 m, and have a limited range and flight duration. Class II (with a maximum take-off weight of 150-600 kg) includes medium-sized UAVs which often use a catapult to take off, and which do not require robust logistic infrastructure. They operate at altitudes of up to 3,000 m. Their equipment includes optoelectronic and infrared sensors, and laser rangefinders. Class III drones (above 600 kg) are the largest UAVs, with the highest take-off weight, and have the longest range and mission duration. Usually they require prepared airfields (landing sites) to take off and land. They are capable of performing various missions thanks to special equipment, which may include radars, lasers and reconnaissance devices. Owing to satellite communication systems, they can carry out tasks in remote regions. They also require appropriate logistic backing. It should be stressed that Class I and II drones are the most common in the public domain, while Class III drones are primarily used by the military, although this is currently no longer a strict rule (The Joint Air Power Competence Centre, 2010: 8).

The main determinants of whether the use of UAVs will be considered possible are the characteristics described by both their benefits and limitations. Their ability to operate in the air for extended periods of time should be viewed as a key advantage associated with the use of UAVs. More specifically, contemporary unmanned aerial platforms are capable of operating in the air (depending on the class) for up to several dozen hours, and the introduction of solar propulsion will extend the UAV mission duration to weeks or even months. Other unquestionable advantages include the safety associated with the pilot (operator) staying outside of the UAV when performing tasks in a hostile environment (contamination, radiation, etc.) and operation flexibility thanks to the use of a wide range of loads (sensors). Due to all these features, one unmanned aerial platform can perform a wide spectrum of tasks.

The potential applications of unmanned aerial systems for civilian purposes may make them useful for two categories of users. The first are state authorities, mainly focused on Class II and III unmanned aerial platforms capable of performing long-term missions. However, under certain conditions, they will also use Class I drones, undoubtedly proving useful in crisis management and as a support in disaster prevention. For example, drones can be used to scrutinise, monitor and analyse a situation in the event of natural disasters such as fires, floods, earthquakes and weather anomalies, as well as to support search and rescue missions. Their role in the protection of critical infrastructure, for instance, in monitoring power plants, gas pipelines, oil pipelines, electricity transmission lines, airports and seaports, etc., is also quite significant, mainly for economic reasons. An important field of application will also be the use of drones providing support for civilian authorities in ensuring internal security: protecting the state border, monitoring mass events or traffic, or supporting police activities in various areas (Skrzypietz, 2012: 18).

The second category includes users of mainly Class I drones for service and commercial activities. In the civilian domain, this should be considered the fastest-developing area, creating new jobs and potential profits for companies using drone technology. This means an increase in the number of drones in public spaces and, by extension, potential security risks.

At present, drones can be used for civilian purposes across several areas related to commercial services. One of these is aerial filming and photography. Bird's eye view shots open up a new perspective and provide viewers with new experiences. The high quality of the recorded images, along with the wide availability of drones, offer substantial opportunities for both amateurs and professionals. Recordings of wedding ceremonies, advertising spots, news media reports, sports broadcasts, music videos, TV programmes or Oscar-winning movies are often shot using drones and they continue to enjoy ample popularity. Due to technological progress and with equipment decreasing in size, it is possible to take professional, high-quality pictures in the traditional 2D technique, and to obtain 3D images, as well as 360-degree pictures with modern technology. In other words, a photo or video camera installed on a drone has become a common working tool.

Virtual reality is another area where drones can be useful. Drones can be used to create spatial 3D scans for games or professional simulators, and not only flight simulators. Their mobility makes it possible to create spatial scans of objects of any height and of large areas. With UAVs, the analysis and documentation of inaccessible places with a large number of obstacles, posing a challenge for manned aircraft, are no longer an issue. Due to the high costs and limited capabilities of manned aviation, even 3D models of airports, which until recently were created using manned aviation, are now being made using drones. The material so acquired is used to create professional flight simulators for training pilots of manned aircraft.

Land surveying is another major field for the commercial use of drones. Drones are capable of recording data for photogrammetric terrain models using "low-altitude" aerial photography. Until recently, photogrammetry and orthophoto maps were created using aerial photographs taken from a manned airplane or helicopter; this is referred to as "medium- and high-altitude" photogrammetry due to its moderate accuracy and high cost. This method is being gradually abandoned. The creation of orthophotos is the main land surveying task carried out using drones. Due to an automatic mission planning option, flight is very precise, saves surveyor's time, and the material so acquired is ready for further processing.

In many regions of the world, drones are already being used in agriculture as well. Modern agriculture is based on what is known as agrotechnology, which refers to all procedures used to cultivate land and plants with a view to producing high yield of the best quality that can be attained. In this field, unmanned aviation is perfect for tasks such as monitoring the vitality of plants, optimising fertilisation and the use of plant protection

products, and crop-dusting on valuable plants where the level of crop damage with traditional fertilisation methods is significant. In the case of any agricultural damage, the material obtained from the air can help to develop a reliable report making it easier to receive compensation for any damage.

Drones are also increasingly used in inspections and environmental protection. Using drones for conducting inspections of buildings, structures, ships, machinery and power lines, as well as performing thermal-imaging measurements of buildings or heat transmission networks, provides accuracy and is safer for people. And due to the high mobility and the ease of performing area observations, drones are also increasingly used for environmental protection. It becomes easier to control the population of forest animals, especially birds. General environmental contamination and the pollution of specific locations can be monitored from the air on an ongoing basis. Moreover, smog, which has become a significant problem in many cities, has prompted another application for drones. An increasing number of measuring devices are intended to be used and mounted on drones in order to monitor the environmental situation.

Also, one should not forget about the use of drones in the transport of various types of shipments. They can also be used to transport samples for analysis, as was the case during the COVID-19 pandemic, or to transport blood between hospitals or deliver medicines to people with impaired mobility. The use of drones for such purposes saves time, especially in crowded cities. In the future, they will also be used to transport people, with a suitably adapted urban infrastructure making this possible.

Drone use for civilian purposes, as discussed above, leads to the conclusion that their number in public spaces will grow significantly. This will raise concerns about the safety of operations performed by them in public spaces, along with related potential threats.

3 Cyber threats connected with the use of drones in public spaces

The use of drones in the public domain may pose certain risks related to the safety of citizens and their property. These can be categorised into several groups. First, technical problems beyond human control which may cause a drone to fall in a place where there are people or elements of their property (buildings, cars, urban infrastructure, etc.). Second, hazards related to human error, considered as non-deliberately contributing to the misuse of a drone or causing it to fail. Third, adverse environmental conditions increasing the likelihood of losing control of the drone, human error or technical failure. Fourth, unpredictable errors and failures which may occur within the infrastructure and any systems supporting UAV operation. Fifth, deliberate human action consisting of an attempt to take control of a drone and use it in an illegal manner. All these categories of hazards contribute to the loss of control of a drone and can consequently lead to the fatal injuries of people, or to property damage both on the ground and in the air (Tran, 2021).

The deliberate use of drones in an illegal manner by a variety of actors (e.g., terrorists or criminal groups) can include physical or cyber-attacks. These cause interference with citizens' privacy and threaten their physical safety. Such activities may include surveillance to track down specific individuals and private areas. The unintentional use of drones, especially over urban areas, can also lead to violations of the law, including the illegal collection of data on people and their property, which may be used for blackmail or fraud. Safety violations can also occur if a drone crashes and hits a built-up area, a parked car or civilians, resulting in property loss and/or damage and human casualties and/or death. What is more, drones are also used to attack guest Wi-Fi and/or short-range Wi-Fi connections, Bluetooth and other wireless devices such as keyboards connected via Bluetooth. Such connections are not protected under the current security measures which assume that nobody can get close enough to breach them or access internal networks using wireless signals. Such assumptions result in poor single-factor authentication and the use of typical passwords which can be easily cracked, especially in the absence of an encrypted connection. This facilitates the interception of information in both private buildings and public spaces (Lee, Eom, Park, & Lee, 2018).

The category of threats associated with deliberately taking control of a drone includes one of the more serious risks associated with drones used in public spaces involving cyber-attacks on specific drone components. This stems from the fact that a drone is only one of the three basic components of the entire system that ensures its functioning (Best, Schmid, Tierney et al., 2020: 15). More specifically, the UAV components include an unmanned aircraft, a ground controller and a communication link. The drone, as an unmanned aircraft, is itself a complex electronic system containing, *inter alia*, a flight controller and navigation devices based on global positioning systems (GPS). The control station provides communication between the ground controller and the station itself, while the communication link ensures communication between the control station and the drone (control and data transfer) (Abid, Austin, Fox, & Hussain, 2014). In other words, an unmanned aerial system can be viewed as an advanced computer containing a wide range of electronic components, a GPS module and communication systems, which may be vulnerable, to a varying extent, to threats involving cyber-attacks. Special attention should be paid to the vulnerability of drone systems to:

a) spoofing: pretending to act as, or disrupting the operation of, the global positioning system (GPS). The lack of encrypted telecommunications links makes it easy for hackers to pretend to act as, jam or disrupt GPS signals. Jamming or disrupting the GPS signal occurs when the hacker is able to generate a stronger signal on the same communication frequency as the one used by a civilian GPS satellite; the drone cannot then receive GPS location information. In consequence, the drone loses its orientation in the air and uses a false location, which may lead to its crashing on the ground (Seo, Lee, Im, Jee, 2015);
b) malware infection. The communication protocols used in drones allow users to pilot them wirelessly using smartphones, tablets or laptops. Nonetheless, this poses the threat of these devices being infected with malware, which may in consequence lead

to taking control of the drone or stealing data collected by the UAV (Kim, Wamper, Goppert, Hwang, Aldridge, 2012: 2438);

c) data interference and interception. Telemetry channels are used to monitor an UAV and to facilitate the transmission of information through open and unsecured wireless transmission, making it vulnerable to various threats. This can result in the interception of data, the implantation of false data and the alteration of pre-established drone airways (Abdallah, Ali, .Mišic´, Mišic´, 2019:43). Moreover, installing or transmitting a number of infected digital files (videos and images) from the drone to the ground station is also possible.
d) manipulation. Since drones generally cover pre-programmed and pre-defined routes, high-value cargo may be exposed to theft, and drones may be diverted to other locations in order to use explosives, biological weapons or other dangerous cargo. All this may happen due to taking control of the drone by, *inter alia*, taking control of or disrupting the GPS signal (Ramon Soria, Bevec, Arrue, Ude Ollero, 2016:700);
e) technical issues. Drones are technical devices which can be vulnerable to all kinds of failures, including application errors such as a loss of connection between the user's control device and the drone, resulting in the drone crashing or being lost. Problems related to the lack of a stable connection, especially under challenging terrain conditions, as well as to battery life, resulting in a very limited flight duration, are also likely to be encountered (Tomislav, Andrija, Jurica, 2018);
f) Wi-Fi jamming. Drones can also be taken over by means of a de-authentication process between the access point and the drone's control device, which can be implemented as a temporary or permanent action, for example, by jamming the drone's operating frequency and redirecting it to the hacker's Wi-Fi connection (Westerlund, Asif, 2019).

The methods presented above involve taking control of the drone or obtaining unauthorised access to data acquired by an UAV. This poses a real danger to people and property in the public domain. Depending on the intentions of the adversary, a drone can be used as a tool for a terrorist attack in a crowded urban area or during a mass event, which may, in consequence, result in a large number of fatalities. A drone can also be used to collect private and sensitive data on specific individuals, which can then be used for blackmail or fraud purposes (Yaacoub, Noura, Salman, Chehab, 2020). As the increasing number of drones in public spaces involves a real danger of unauthorised use, there is a need to counter such incidents.

4 Counteracting threats involving the unauthorised use of drones in public spaces

The issue of ensuring the security of drone operations in public spaces requires a comprehensive approach. It should include the following: a) relevant legal regulations; b) prevention; c) the readiness of dedicated services and resources to counter threats; d)

the detection, identification and neutralisation of drones posing threats; and e) gathering experience.

Legal regulations provide the basis for the appropriate and lawful use of drones in public spaces. Current legislation allows drones to be used in urban areas under certain conditions. Drone users must hold the required licences, and drones should be registered so that they can be identified and, when necessary, that those who use UAVs in violation of the law can be held liable. The second component, i.e., prevention, should focus on raising awareness among drone users of the risks associated with their use. This entails the need for drone users to obtain specific authorisations, acquired through training, along with appropriate licences authorising them to use drones. In addition, it is necessary to hold responsible any persons who deliberately use drones in an unlawful manner. The inevitability of punishment, including the confiscation of equipment or the suspension or revocation of licences for life, should make users aware of the real risks associated with drones used in public spaces. Information campaigns for both drone users and society at large that should be aware of the dangers associated with the operation of drones in public spaces should constitute an important element of the aspect in question. This also involves the need for decision-makers to have social acceptance for drone operations conducted in public spaces. Only then will it be possible to develop drone technology for economic and social needs. The third component concerns the readiness to use appropriate force and resources to prevent any threats connected with drones used in public spaces. This readiness should be based on the developed risk scenarios and risk prevention procedures for UAVs (Majeed, Abdullah, Mushtaq, Kazmi, 2021). Furthermore, exercises of crisis management teams should be conducted, and these should be based on scenarios taking into account the risk of using drones in an illegal manner in the public domain. Well-prepared services should also have technologies to respond appropriately to a given situation. Another aspect involves activities aimed at physically responding to the threats connected with the unauthorised use of drones in public spaces. It includes detecting, identifying and possibly neutralising drones that are used in public spaces in an illegal manner. Detection may include the use of multiple technologies to track down a drone in airspace. These technologies are: radars, passive radio frequency identification systems, optoelectronic systems, active optical systems, magnetic detection and acoustic detection systems, as well as watchers. The best outcomes are achieved by combining several drone detection methods. Identification, in turn, should ensure the confirmation that a drone being used in an illegal manner has been detected and the specific risk has been defined. Another aspect is the neutralisation of drones posing threats in public spaces. The neutralisation can be either passive or active. Passive neutralisation may include the use of barriers, nets or physical fences in selected public spaces. Geofencing should also be used, which is a limiting feature within a drone, preventing it from going beyond pre-defined zones in public spaces. In the future, dynamic geofencing will also be used, making it possible to react, in real time, to drones penetrating prohibited areas within the public domain. Active neutralisation, by contrast, involves the physical neutralisation of drones in public spaces. This may consist in jamming radio links, taking control of a drone, intercepting it and, as the last-case scenario, shooting it down. Such neutralisation

requires the provision of security measures for people and property within the impact zone. The comprehensive approach to counteracting threats related to the use of drones in an unauthorised manner ends with "lessons learned" – conclusions to be gathered and incorporated in relevant legal regulations and procedures.

This comprehensive approach also includes the use of cyber defence technologies in relation to drones posing threats in public spaces. These operations are implemented in an identical manner as those undertaken by people intending to use drones in an unlawful manner, the only difference being that such measures are carried out by the relevant services acting in accordance with the law. However, the tools that are used in cyber defence are virtually the same.

5 Summary

The use of drones in public spaces can undoubtedly be expected to increase in the near future. The potential of drones, on the one hand, cannot be overestimated when it comes to the functioning of many spheres of social and economic life. On the other hand, their operation in public spaces poses threats to the safety of people and property. Therefore, the first thing to do should be to develop a map of threats to specific public spaces within which drones will perform operations in the future and to establish an effective plan to neutralise any identified risks. The identification of security gaps in the components used for drone production, as well as in software used for their operation, is another aspect that should be taken into consideration. This requires the constant monitoring of the UAVs systems and keeping pace with technological development. It is no less important to invest in regular equipment tests as part of cross-sectoral cooperation (involving the state, private companies, laboratories, research centres, etc.), as in this way, it is possible to develop universal safety and security protocols which could be implemented on a wider scale. It also seems indispensable to ensure coordinated and constantly updated monitoring and intervention systems, as even cutting-edge solutions do not offer full immunity against all cyber-attacks. In this respect, it will be necessary to strengthen the cooperation between producers of UAV components, state administration authorities and services responsible for broadly defined security and public order.

References:

Abdallah, A., Ali, M.Z., Mišic,´ J. & Mišic´, V.B. (2019) Efficient security scheme for disaster surveillance uav communication networks, *Information*, 10(2), pp. 1-22.

Abid, M.E, Austin, T., Fox, D. & Hussain, S.S. (2014) *Drones, uavs, and rpas: an analysis of a modern technology* (Worcester, Massachusetts: Worcester Polytech. Inst.).

Best, K.L., Schmid, J., Tierney, S., Awan, J., Beyene, N.M., Holliday, M.A., Khan, R. & Lee, K. (2020) *How to Analyze the Cyber Threat from Drones* (Santa Monica: RAND Corporation).

Kim, A., Wampler, B., Goppert, J., Hwang, I. & Aldridge, H. (2012) Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, *Infotech@ Aerospace*, 2012, pp 1-30.

Lee, H., Eom, S., Park, J. & Lee, I. (2018) Uav-aided secure communications with cooperative jamming, *IEEE Transactions on Vehicular Technology*, 67(10), pp. 9385–9392.

Majeed, R., Abdullah, N.A., Mushtaq, M.F. & Kazmi, R. (2021) Drone Security: Issues and Challenges, *International Journal of Advanced Computer Science and Applications*, 12(5), pp. 720-729, https://doi.org/10.14569/IJACSA.2021.0120584.

Ramon Soria, P., Bevec, R., Arrue, B., Ude, A. & Ollero, A. (2016) Extracting objects for aerial manipulation on uavs using low-cost stereo sensors, *Sensors*, 16(5), pp. 1-19.

Seo, S.-H., Lee, B.-H., Im, S.-H. & Jee, G.-I (2015) Effect of spoofing on unmanned aerial vehicle using counterfeited gps signal, *Journal of Positioning, Navigation, and Timing*, 4(2), pp. 57–65.

Skrzypietz, T. (2012) Unmanned Aircraft Systems for Civilian Missions, *Policy Paper*, (1) (Potsdam: Brandenburg Institute for Society and Security).

The Joint Air Power Competence Centre (2010) *Strategic Concept of Employment for Unmanned Aircraft Systems in NATO* (Kalkar: NATO).

Tomislav, R., Andrija, V., Jurica, I. & Bo, W. (2018) Challenges and solutions for urban uav operations, *International Scientific Conference "Science and Traffic Development"(ZIRP 2018)*, available at: https://www.bib.irb.hr/938317/download/938317.Radii_Vidovi_Ivoevi_Wang_Challenges_and_Solutions_For_Urban_UAV_Operations.pdf (August 31, 2022).

Tran, T.D. (2021) *Cybersecurity risk assessment for Unmanned Aircraft Systems*, available at: https://hal.archives-ouvertes.fr/tel-03200719v2 (August 30, 2022).

Westerlund, O. & Asif, R. (2019) Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things, *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*, (IEEE), pp. 1-10.

Yaacoub, J.P., Noura, H., Salman, O. & Chehab, A. (2020) Security analysis of drone systems: Attacks, limitations, and recommendations, *Internet of Things*, 11, pp. 1-39, https://doi.org/10.1016/j.iot.2020.100218.

The Importance of Communication and Information Systems for the Operation of Systems Controlling the Movement of Cultural Assets - Selected Issues

KATARZYNA ZALASIŃSKA

Abstract After 2015, the illegal movement of cultural assets has been identified by the international community as one of the main sources of funding for international terrorism. This paper discusses selected issues related to the introduction of information exchange tools at European Union and national levels, with particular focus on the importance of systems for controlling the legality of the movement of cultural assets at the Ukrainian border. Electronic tools and systems have the potential to enhance cooperation, but they cannot replace it. The emphasis therefore should be up on building specialised human resources and creating the conditions for their cooperation in an international environment. The VINCI II system is an electronic database system for collecting data on permits for the permanent and temporary overseas export of monuments. Authorities issuing permits for the permanent and temporary export of antiquities abroad enter scans of these export decisions into a system, subsequently accessed by law enforcement authorities, including the Police, the National Tax Administration, the Border Guard and conservation services. The VINCI II system enables the rapid and efficient exchange of information on the movement of cultural property.

Keywords: • cultural assets • communication • information systems • VINCI II

CORRESPONDENCE ADDRESS: Katarzyna Zalasińska, Ph.D., Associate Professor, University of Warsaw, The Faculty of Law and Administration, Ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa, Poland, e-mail: kasiazalasinska@op.pl, ORCID 0000-0003-2171-2560.

https://doi.org/10.4335/2022.2.10 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

After 2015, the illegal movement of cultural assets has been identified by the international community as one of the main sources of funding for international terrorism. The contemporary battle against international terrorism is also therefore necessary for countering crimes against heritage. Therefore, concerns regarding global security have been added to the catalogue of threats related to the protection and integrity of the cultural heritage of countries where cultural assets originate from. The activity of international organisations has resulted in legal developments both at the level of the European Union and individual national legislations. In the context of the changes that have been introduced in recent years, the importance of communication and information systems for ensuring the effectiveness of such systems for controlling the movement of cultural assets has increased significantly. This paper discusses selected issues related to the introduction of information exchange tools at European Union and national levels, with particular focus on the importance of systems for controlling the legality of the movement of cultural assets at the Ukrainian border.

A milestone for the international community to intensify its commitment to ensuring effective control over the movement of cultural assets was the UN Security Council Resolution 2199/2015 of 12 February 2015 (S/RES/2199 (2015)) and Resolution 2347/2017 of 24 March 2017 (S/RES/2347 (2017)). Resolution 2199/2015 requires UN Member States to undertake measures to prevent terrorist groups from raising funds from, inter alia, the trafficking of antiquities, as well as to take appropriate measures, in cooperation with Interpol, UNESCO and other international organisations, aimed at preventing the trafficking of objects of cultural, scientific and religious value from Iraq and Syria, and to enable the safe return to their countries of origin. Resolution 2347/2017, for the first time, explicitly indicated that the protection of cultural assets is one of the areas for ensuring global peace and security throughout the world. This was the first UN Security Council Resolution addressing the protection of cultural assets in relation to contemporary threats, and its intention was to highlight the role of the UN and its institutions, in particular UNESCO, for securing endangered monuments. Like before, states were obliged thereunder to adopt measures to combat the illegal trafficking of cultural assets, as well as to undertake extensive international cooperation in this field. The European Union's response to the challenges identified was to undertake legislative work, resulting in Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the entry and the import of cultural assets. Beforehand, taking into consideration Council Conclusions of 12 February 2016 on combating the financing of terrorism and communication from the Commission to the European Parliament and the Council of 2 February 2016 on an Action Plan for strengthening the combat against the financing of terrorism, as well as Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ EU L 88, 31.3.2017, p. 6), it is necessary to adopt common rules on trade with third countries to ensure effective protection against the illicit trafficking of cultural assets and against their loss or destruction, to safeguard the cultural heritage of mankind and to

prevent the financing of terrorism and money laundering from the sale of seized cultural assets to purchasers in the Union. The proposal to adopt new EU legislation with direct effect was presented by the European Commission in 2017 as part of the implementation of the European Security Agenda and Action Plan to intensify the combat against terrorist financing.

When preparing Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the entry and import of cultural assets (OJ EU L 151, 07.06.2019, p. 1), it was understood that, considering the different rules applied in Member States to the importing of cultural assets into the customs territory of the Union, measures should be taken, in particular, to ensure that the importing of certain cultural assets shall be subject to uniform controls when they enter the customs territory of the Union. This should be carried out following existing processes, procedures and administrative tools to achieve uniform implementation of Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 establishing the Union Customs Code (OJ EU L 269, 10.10.2013, p. 1. In this context, it should be recalled that the protection of cultural objects recognised as national treasures of the Member States was previously covered by Council Regulation (EC) No 116/2009 of 18 December 2008 on the export of cultural assets (OJ EU L 39, 10.2.2009, p. 1) and Directive 2014/60/EU of the European Parliament and the Council of 15 May 2014 on the return of cultural assets unlawfully removed from the territory of a Member State, amending Regulation (EU) No 1024/2012 (OJ EU L 159, 28.5.2014, p. 1). Accordingly, this Regulation should not apply to cultural assets which originate, or were discovered, in the customs territory of the Union. The common rules introduced should cover the customs clearance of cultural assets from outside the Union introduced into the customs territory of the Union. Furthermore, it is accepted that for the purpose of the present Regulation the relevant customs territory should be the customs territory of the Union at the time of importation.

Under the approved 2019 Regulation, considering that certain categories of cultural assets, mainly archaeological sites and elements of monuments, are particularly vulnerable to looting and destruction, it was deemed necessary to introduce a system of enhanced inspections before they are allowed to enter the customs territory of the Union. Such a system should require the presentation of an import licence issued by the competent authorities of a Union Member State before such cultural assets are released for marketing in the Union or placed under a special customs procedure other than transit. Regarding categories of cultural assets the importation of which does not require an import licence, the Regulation accepts that persons intending to bring such goods into the customs territory of the Union should, by means of a declaration, certify and assume responsibility for their lawful export from a third country and should provide sufficient information on cultural assets to enable them to be identified by customs authorities. To facilitate the procedure and for reasons of legal certainty, information on cultural assets should be provided using a standardised document. As recommended therein, the Object ID standard (https://icom.museum/en/resources/standards-guidelines/objectid/),

promoted by UNESCO, could be used to describe cultural assets. Particularly pertinent to the subject of this paper is the fact that the holder of the assets is expected to record this information in an electronic system in order to facilitate identification by customs, to enable risk analysis and targeted controls, as well as to guarantee the traceability of the cultural assets once they have entered an internal market.

According to the Regulation, the European Commission shall be responsible for establishing a centralised electronic submission system for import licence applications and importers' declarations, as well as for storing and exchanging information between Member States' authorities, more specifically with regard to importers' declarations and import licences. The system is to become operational by 2025 at the latest.

The Regulation itself does not provide detailed information on an electronic system. The only indication provided is that it is intended both for the submission of applications and for the exchange of information between competent authorities. The Regulation also states that data processing should be able to include personal data and should be performed in accordance with the Union law. Member States and the Commission should process personal data only for the purposes thereof or in duly justified circumstances for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and prevention of threats to public security. Any collection, disclosure, transmission, communication and other processing of personal data made within the framework the Regulation should be subject to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (The General Data Protection Regulation) (OJ EU L 119, 4.5.2016, p. 1 and (EU) 2018/1725 1725 of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ EU L 295, 21.11.2018, p. 39). The processing of personal data for the purposes thereof should also be in compliance with the rights to respect for private and family life as recognised in Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms as well as with the right to respect for private and family life and the right to the protection of personal data as recognised in Articles 7 and 8, respectively, of the Charter of Fundamental Rights of the European Union. The protection of personal data has been set out in Article 10 thereof. Customs authorities and the competent authorities of Member States shall act as the controllers of personal data obtained pursuant to Articles 4, 5 and 8 of the Regulation. The processing of personal data thereunder shall be limited to the purposes laid down in Article 1 (1) therein. Only duly authorised staff of the authorities shall have access to personal data obtained pursuant to Articles 4, 5 and 8 thereof, and such data shall be appropriately protected against unauthorised access or communication. The data may not be disclosed or transmitted without the express written consent of the authority that

originally obtained it. However, such consent shall not be necessary where the authorities are obliged to disclose or transmit data pursuant to the provisions in force in the Member State concerned, particularly in connection with legal proceedings. The authorities shall retain any personal data obtained in accordance with Articles 4, 5 and 8 for a period of twenty years from the date of their acquisition. Upon expiry of that period such personal data shall be deleted.

The Regulation stipulates that an information system shall not only serve administrative processes, but also the international exchange of information between operators. Information on the movement of cultural assets is to be collected in electronic form. Under the Regulation, they are to be exchanged between Member States and the Commission in order to support the effective implementation thereof and provide a basis for its future evaluation. To ensure the transparency of this data collection, as much information as possible should be made public. However, this issue is not specified any further in the Regulation, which may raise some uncertainties at the future stage of application.

Pursuant to Article 8, which refers to an electronic system, it has been accepted that the storage and the exchange of information between Member States' authorities, in particular with regard to import licences and importers' declarations, shall be carried out by means of a central electronic system. In the case of temporary failure of the electronic system, other means of storing and exchanging information may be used in a provisional manner. Pursuant to Article 8(2), the Commission is required to define, by means of implementing acts, rules for the implementation, operation and maintenance of an electronic system referred to in Paragraph 1 and to provide detailed rules relating to the submission, processing, storage and exchange of information between Member States' authorities using an electronic system or other means referred to in Paragraph 1. These implementing acts were adopted on 24 June 2021 (Commission Implementing Regulation (EU) 2021/1079 of 24 June 2021 laying down detailed rules for implementing certain provisions of Regulation (EU) 2019/880 of the European Parliament and of the Council on the introduction and the import of cultural goods (OJ EU L 234, 2.7.2021, pp. 67-89). The date mentioned is important in that, according to Article 9, the Commission is obliged to set up an electronic system which needs to be operational at the latest four years after the entry into force of the first mentioned implementing act.

To summarise the above discussion, it should be noted that the primary objective of the Regulation was to define the conditions for the entry of cultural assets into the Community. While the previously adopted provisions applicable to the control of the export of cultural assets outside the Community were introduced in view of the security of trade and the associated risks to cultural heritage, the 2019 Regulation was based on the issue of preventing the illegal trade in cultural assets, especially where such trade could contribute to the financing of terrorism. Moreover, it is worth emphasising that the Regulation makes the creation of an electronic system a prerequisite for the entry into

force of individual provisions. Meanwhile, the Commission has been given four years to develop such a system, adjusting to the level of implementing legislation and the rules on the implementation, operation and maintenance of an electronic system. It would appear that the launch of an electronic system six years after the adoption is a long time to wait to start the actual functioning of a system for controlling the movement of cultural assets so that both the core assumptions and the detailed arrangements (including Annex C) may undergo amendment. It should be anticipated that the Regulation will need to be updated before 2025. It is worth noting, for example, that in an era of the dynamic development of new technologies, it is impossible to predict in advance what the possibilities for the development of electronic systems will be.

As a complement of the above discussion, it is worth transferring the discussed issues to a national level. In this regard, it is worth presenting the use of electronic systems and tools, including the exchange of information between authorities adopted in Poland. An example of such measures may be the VINCI II system launched in Poland in 2021. The further part of this paper will provide a brief outline of the operation of this system.

The VINCI II system is an electronic database system for collecting data on permits for the permanent and temporary overseas export of monuments. Authorities issuing permits for the permanent and temporary export of antiquities abroad enter scans of these export decisions into a system, subsequently accessed by law enforcement authorities, including the Police, the National Tax Administration, the Border Guard and conservation services. The VINCI II system enables the rapid and efficient exchange of information on the movement of cultural property.

Therefore, to describe the operation of this system, it is necessary to provide a brief outline of the currently applicable regulations. According to the Act on the Protection and Care of Historical Monuments, the permission for the permanent and temporary export of historical monuments abroad is granted by the Minister of Culture and National Heritage and the Voivodship Conservators of Historical Monuments, respectively. These decisions are made on paper and current legislation does not allow proceedings to be conducted electronically. Therefore, it is impossible for information to circulate rapidly between authorities. Paper-based proceedings prevent the competent authorities from quickly and effectively verifying documents and the legality of the export of cultural assets abroad. Moreover, experience indicates that export documents themselves are often forged or falsified, which further raises the necessity to verify the reliability of documents presented during inspections.

The objective of the VINCI II system is to adopt tools, based on existing technical solutions, for the electronic recording of decisions on permits for the permanent and temporary export of antiquities abroad and, consequently, of data on exported objects. Furthermore, additional documents will be stored in the database (e.g., reports on the inspection of an object, which is performed before the issuance of a permit). In this

system, it is possible to search for an export permit using a search engine by entering, for example, the author, the title of the work of art, its name, the permit number or the date of issue. Gathering data on trade in this manner, as well as providing easy access for authorised entities, will undoubtedly contribute to the strengthening of security in the area of the trade in works of art by prompt and effective verification by competent authorities (border guards, the National Fiscal Administration, the police) of permits issued for the export of antiquities abroad.

The VINCI II programme provides an example of searching for new tools to optimise the performance of public administration. Finally, it is the first step towards a change in the administration model within the heritage conservation field, which in the future should make greater use of electronic systems. However, it is worth emphasising that this project has been implemented without the need to amend current legislation. Indeed, it was an example of a paradigm shift to make the export control system more efficient by providing tools for the rapid exchange of information, which is crucial for the movement of assets. This is an example of interoperability and cooperation based on bilateral agreements, which is acceptable at the level of the authorities.

These two examples of the use of electronic systems represent two differing approaches to their meaning and function. Regarding the VINCI II system, it is assumed that the performance of the control system, including through the issuing of permits, is not conditional on the creation of electronic tools. The adopted proceedings are conducted in paper-based form. The system created to support public administration authorities, on the other hand, is an example that, despite the maintenance of paper form proceedings, it is possible to ensure increased efficiency of export controls through the use of modern electronic tools. Another example is the creation of an electronic system, described in the introduction and provided for in Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the entry and import of cultural assets, which supports applications but also allows the exchange of information between relevant entities. There are particular doubts as to the length of time required for the implementation of the regulation and the fact that its entry into force is conditional on the achievement of efficiency in an electronic system, the rules for the implementation, operation and maintenance of which were laid down two years after the adoption of the regulation. Accepting such a long period between the adoption of the Regulation and the commencement of its operation in its entirety means that it may prove to be inadequate to the challenges and problems of trading. It would therefore appear that, where the achievement of the performance of an electronic system is specified as a condition for the enactment of legislation, resolving basic implementation issues should precede the adoption of the regulations under which the systems are to operate. Consideration should also be given as to whether an electronic system is always to be a condition for the functioning of the rules (e.g., when the obligation to operate in an electronic system should apply to citizens) or a tool used by the administration during the implementation phase (aimed at increasing the efficiency of tasks by means of closer cooperation between

state bodies). In conclusion, the key to the effectiveness of legislation is the cooperation of authorities and institutions. Evidently, electronic tools and systems have the potential to enhance cooperation, but they cannot replace it. The emphasis therefore should be up on building specialised human resources and creating the conditions for their cooperation in an international environment.

References:

Konwencja Rady Europy o ochronie praw człowieka i podstawowych wolności, 4 listopada 1950 (Dz. U. z 1993 r. nr 61, poz. 284).

Rozporządzenie Rady (WE) nr 116/2009 z dnia 18 grudnia 2008 r. w sprawie wywozu dóbr kultury (Dz.U. L 39 z 10.2.2009, s. 1).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 952/2013 z dnia 9 października 2013 r. ustanawiające unijny kodeks celny (Dz.U. L 269 z 10.10.2013, s. 1).

Dyrektywa Parlamentu Europejskiego i Rady 2014/60/UE z dnia 15 maja 2014 r. w sprawie zwrotu dóbr kultury wyprowadzonych niezgodnie z prawem z terytorium państwa członkowskiego, zmieniająca rozporządzenie (UE) nr 1024/2012 (Dz.U. L 159 z 28.5.2014, s. 1.

Rezolucja Rady Bezpieczeństwa ONZ nr 2199/2015 z 12 lutego 2015 r. (S/RES/2199 (2015).

Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 28 kwietnia 2015 r. Europejska Agenda Bezpieczeństwa COM (2015) 185 final.

Konkluzje Rady z dnia 12 lutego 2016 r. w sprawie zwalczania finansowania terroryzmu Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 2 lutego 2016 r. w sprawie planu działania na rzecz skuteczniejszego zwalczania finansowania terroryzmu.

Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 2 lutego 2016 r. w sprawie planu działania na rzecz skuteczniejszego zwalczania finansowania terroryzmu COM(2016) 50 final.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

Karta praw podstawowych Unii Europejskiej (Dz. U. UE C 202 z 7.6.2016, p.389 – 4-5).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).

Rezolucja Rady Bezpieczeństwa nr 2347/2017 z 24 marca 2017 r. (S/RES/2347 (2017).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/880 z dnia 17 kwietnia 2019 r. w sprawie wprowadzania i przywozu dóbr kultury (Dz. Urz. UE L 151 z 07.06.2019, str. 1).

Commission Implementing Regulation (EU) 2021/1079 of 24 June 2021 laying down detailed rules for implementing certain provisions of Regulation (EU) 2019/880 of the European Parliament and of the Council on the introduction and the import of cultural goods (Dz.U. L 234, 2.7.2021, p. 67–89).

Object ID standard, available at: https://icom.museum/en/resources/standards-guidelines/objectid/ (August 30, 2022).

From Facebook to Telegram - The Migration of Radical and Anti-vaccine Groups Across Digital Platforms

AGNIESZKA LIPIŃSKA

Abstract After exposing the impact of Cambridge Analytica on the outcome of the 2016 US election, and due to the growing activity of terrorists and radical groups using this medium, both public and state authorities have begun to put more pressure on social media to control and regulate content disseminated via these platforms. This has made the online activities of groups disseminating controversial content more diverse. Recently, the Telegram instant messaging platform has become the most popular medium used to promote such content.

Keywords: • QAnon • anti-vaccination groups • ISIS • information bubbles • social protests • Facebook • Telegram

CORRESPONDENCE ADDRESS: Agnieszka Lipińska, Ph.D. student, War Studies University in Warsaw, Faculty of National Security, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: lipinskaagnieszka065@gmail.com, ORCID: 0000-0003-3108-8095.

https://doi.org/10.4335/2022.2.11 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

The opportunity to establish contacts and to share interests and passions with people from all over the world has been, for many years, considered the advantage of Facebook and other social media, as well as the main reason for their immense popularity. Thematic groups, both professional and private, make it possible to exchange views, to update knowledge and to get to know people we would never meet if we were not internet users. Social groups focusing on passions, parenting, interior design, culture, tourism or the automotive industry constitute platforms for the exchange of ideas and experiences, and they often provide support for people struggling with various problems (which was particularly visible in the initial period of the struggle against COVID-19 when, for example in Poland, due to the lockdown, the number of thematic and self-assistance groups increased, including Kultura w kwarantannie *(Culture in Quarantine)* or Widzialna Ręka *(A visible hand)*, the latter referring by its name to the popular 1980s TV programme Niewidzialna Ręka *(An invisible hand)*, in which help was secretly provided to those in need, usually the elderly). Closed groups are created for people with eating disorders, for adoptive parents and single people. Their users ensure a friendly atmosphere of the discourse by reporting inappropriate posts to the administrators. Such communication and support patterns create a sense of community and often play a therapeutic role.

For several years however, and especially since the Cambridge Analytica scandal in the United States came to light in 2018, the activities of some groups established on Facebook and other social media, as well as the content they publish, have been under strong criticism. The use which Cambridge Analytica made of the knowledge about individuals, their affiliations, political views and value systems resulted in attempts to influence their political choices through personalised and carefully crafted messages. Social engineering applied on such a large scale for the first time resulted in Trump's victory in the 2016 presidential election in the USA. At the same time, it made a large part of the population realise that there are some mechanisms behind the choice and the display of content on the "wall", and that being closed and functioning within what is known as information bubbles has some adverse effects. In addition, this was confirmed by the so-called Facebook papers revealed by F. Haugen in October 2021. These were internal Facebook documents (Pierce, Kramer, 2021) showing that the algorithms of the platform are designed to evoke emotions and *de facto* polarise society. Although, in consequence of the feeding frenzy in 2017, the company declared that it would both abandon the meticulous profiling of its users and fight down hate speech and disinformation, its actions in this regard have proven insufficient. The results of the internal audit that Facebook committed to conduct at that time were not announced (in October 2019, the company made a settlement with the UK data protection supervisory body, agreeing to pay in full the £500,000 fine imposed by the ICO in 2018 in connection with the activities of Cambridge Analytica. https://techcrunch.com/2021/01/26/facebooks-secret-settlement-on-cambridge-analytica-gags-uk-data-watchdog/In January 2021, the UK Information Commissioner admitted that her office, under a secret agreement with Facebook, would not provide a parliamentary subcommittee with information on whether

it had actually completed that audit or not. Nor has any report been published to show the real impact of the audit or changes to its privacy policy; instead, lobbying efforts have been intensified).

The disturbing consequence of functioning within an information bubble has been confirmed by studies conducted in many countries, focusing on the spread of disinformation on the internet concerning COVID-19 and the side effects of vaccinations against this disease. Although M. Zuckerberg has officially vowed to fight down disinformation on his social networking platform (as in the case of content disseminated via YouTube), such actions are limited and fail to bring the expected outcomes. Many groups and profiles that have been closed down are re-established under a different name or move some of their banned activities to different communication channels. As reported by NBC News (Collins, Zadrozny, 2021), attempts by US users to deceive Facebook algorithms take increasingly sophisticated forms. Groups (mostly private or hidden) spreading radical or conspiratorial views often use names completely unrelated to their subject matter. After the events in Charlottesville in 2017, with a right-wing radical murdering Muslims, a group for ultra-right-wing users changed its name to "Muslims for Peace". The anti-vaccine community operates in a similar manner, using such names for their groups as "Dance Party" or "Dinner Party". It also uses neutral key words/codes to hide messages from the algorithms that track down disinformation, with Pfizer's vaccination being referred to as "pizza" and Moderna's as "Moana" (Similar coding was previously used, for instance, by Islamic terrorists). This shows that the fight against this type of action fails to bring satisfactory outcomes. In the English-speaking space on the internet (Instagram, Twitter, YouTube and Facebook), more than 400 accounts were involved in transmitting and disseminating information to 58 million followers in 2019-2020 (Center for Countering Digital Hate, 2021). In Poland, according to a study of online activity conducted by A. Mierzyńska in January 2021, the 25 most active accounts and channels for disseminating anti-vaccination information on Facebook and YouTube had 1.66 million followers (Mierzyńska, 2021).

The 6 January 2021 events, and more specifically the attack on the US Capitol, clearly proved the impact power vested in groups that are united by a common mission. The above-mentioned storming of the US Congress shows how powerful it is to function within a certain cognitive paradigm and in a group that follows the same views. Representatives of the QAnon movement, who had previously gathered online, interrupted the session devoted to approving the results of the US election (and, more specifically, Joe Biden's victory), with four people being killed as a result of these protests. QAnon representatives were united by the thesis that only Trump could be the real president of the USA and only he would be able to lead the fight against the secret criminal organisation ruling the USA (supposedly including H. Clinton). However strange it may sound, the movement is very robust and gathers followers of various conspiracy theories, including right-wing extremists and anti-vaccinationists. Its members stigmatise certain journalists and politicians, encouraging their punishment and,

due to its radical attitude, the movement is becoming increasingly popular. Among its followers is Marjorie Taylor Greene from the US House of Representatives. The QAnon movement is also present in Europe, and its supporters have a variety of affiliations, ranging from the extreme right to declared anti-vaccinationists and so-called normal citizens susceptible to conspiracy theories.

The methods used to counteract the groups that create harmful information bubbles and spread disinformation and conspiracy theories have proven ineffective. These communities are capable of re-establishing their activities under new names, or they begin to diversify their content, moving to new communication platforms in order to reduce the risk of being targeted/excluded. The QAnon movement, as well as radical right-wing and anti-vaccination groups, have been present on Facebook and YouTube, to a lesser extent on Twitter, and for a few years also on Telegram.

Given their long-standing on-line presence and know-how about using the internet for propaganda purposes, terrorist groups best reflect these tendencies. According to researchers dealing with this subject matter, while ISIS was mainly present on Facebook between 2015-2017, they had already began to expand their activities to other social media platforms, including Telegram. This was confirmed by a study (Ayad, 2020) of the functional structure of the ISIS propaganda distribution channel on Facebook based on the example of the Fuouaris Upload network. With 90 main accounts, another 288 were affiliated, constituting a group of friends and followers of Arabic language users and, at the same time, running their accounts and distributing material to their separate groups created in local languages, such as Indonesian, Ethiopian, Somali, Bengali and Albanian. M. Ayad referred to these types of structures as expanding networks within networks. At the same time, ISIS had already been moving most of its operations to Telegram for several years, and the peak popularity of this instant messaging platform among ISIS supporters was recorded in 2017-2018.

A similar scenario was observed among groups of right-wing extremists. They had been previously active on Facebook or created their own websites or fora. The most famous entity running its online services for the radical right was the Seattle-based company Epik. It registered domains and hosted far-right and neo-Nazi websites, including those which other providers had refused to serve (it also served the radical group 8chan). It is the group behind Parler (which was intended both to serve as a response from right-wing circles, mainly from the USA, to restrictions imposed by Facebook and to guarantee freedom of expression and the unrestricted exchange of ideas and beliefs, now operating in a limited form), which intensified its fight against right-wing propaganda after the attack on the Capitol in 2021. In October 2021, hackers from the Anonymous group revealed a massive leak of passwords, user data and phone numbers of people using Epik services. Both that leak and the aforementioned actions by Facebook related to the QAnon movement resulted in a large part of such groups and right-wing network users being transferred to Telegram.

At present, due to increasing pressure from the authorities and law enforcement in various countries, major technology companies take measures to fight down hate speech and to detect radical content on the web more efficiently. In addition, instant messaging platforms impose certain restrictions as to the number of group members. Telegram becomes a suitable choice for those wishing to bypass these restrictions. Along with the afore-mentioned ability to diversify information distribution channels, it is currently the least controlled medium. It is a mobile app with a range of mass communication features, as well as encrypted chat and file sharing options. Following the storming of the US Capitol on 6 January 2021, Telegram announced that it had gathered more than 500 million active users worldwide. The app is becoming increasingly popular also among American users. According to data from Sensor Tower, a company dealing with app measurements, Telegram downloads in the USA are growing significantly, with the platform becoming particularly attractive to QAnon supporters and right-wing extremists (Khan, 2021). This growth in popularity is also linked to the WhatsApp privacy update (the WhatsApp and Facebook crash of October 2021 resulted in more customers).

Telegram was founded by P. Durov, a Russian computer scientist and creator of the social networking platform VKontakte. A journalistic investigation conducted by Spiegel (Hebel, Hoppenstedt, Rosenbach, 2021) revealed that the owner of this instant messaging platform had created a network of companies registered in Belize and the Virgin Islands, and that it was difficult to get answers to letters about potentially dangerous users from a company registered in Dubai.

Telegram consists of three main components:
1 – channels – both public and private (most of which are one-way transmissions) that can be followed by an unlimited number of people;
2 – groups – public and private, in which up to 200,000 people can communicate (larger groups are faster and more powerful).;
3 – secret chats allowing individual end-to-end encrypted conversations, which makes it impossible for the police and services to discover the content of correspondence. It is also possible to delete messages displayed to all participants in a conversation. In addition, it has the option to enable an automatic deletion timer (to delete messages after a certain period, e.g., after 24 hours or a week) in each selected conversation (this is particularly important for some users as, for instance, the non-deleted records of a conversation between the participants in the 2016 military coup in Turkey made it easier to detect its members).

Contrary to other platforms, the app allows file storage, which makes it a very attractive medium for extremists distributing radical recordings and manifestos through it, and its worldwide popularity gives them the opportunity to attract wide audiences. Telegram provides the ability to share a wide range of files, including photos, audio messages and videos, sized up to 1.5 GB. Although the terms and conditions of using the service

prohibit the popularisation of violence in public channels, they make no mention of doing so via private channels or groups. The rules of content moderation also remain unclear. Recently, there has been evidence of more active content moderation on Messenger – since 2019, in cooperation with Europol, the company has been removing some channels that promote terrorism (e.g., distributing information on the production of home-made bombs). However, it is still possible to find some material containing ISIS propaganda. In addition to disseminating any content via the group which concerns maintaining cyber security and low-profile attacks, it maintains channels propagating a radical Salafist version of Islam.

Right-wing extremist groups, like the American Proud Boys (a neo-fascist group founded in 2016), are also present on the instant messaging platform in question. The nonchalant or libertarian approach previously taken by its owner as regards the presented content also attracted Darknet vendors – Telegram's black market offers hacking services, sales of documents, drugs, etc. A separate user category is made up of pan-Slavic/nationalist groups bringing together Ukrainians from the Azov Battalion and Polish right-wing nationalists containing hate speech and praise for the supremacy of the white race. It also contains some anti-Ukrainian channels glorifying the Slavic Polish-Russian brotherhood (the author of one of these, Horus, in the description of his Twitter account, which abides by stricter restrictions, provides the following information about the content of his channel on Telegram: Due to the faulty system of material verification, I will be posting some/all of the content disputable for the "community" on (...) - *I deliberately do not give the address of the channel*). The European Eastern Resistance Movement, which promotes the activities of the so-called Waffen Division (a dangerous neo-Nazi group broken up in 2018, the reactivation of which was reported at the beginning of 2021), Extinction Rebellion and the Polish Rodacy Kamraci anti-vaccinationists also post their content there.

Channels and chats propagating violence and pornography also appear on the platform – in October 2021, The Male State (Мужское государство) channel, which demeaned, mocked and encouraged the persecution of gay men, feminists and women having relationships with dark-skinned men and men from Caucasus by publishing their addresses, photos and phone numbers, was shut down. Members of the group met to train in hand-to-hand fighting and shooting (Davidovic, 2021).

Following a journalistic investigation conducted in 2021, Telegram also shut down several dozen Korean chatrooms whose users had access to videos of under-age girls being forced into self-harm and sexual acts. These often included girls' names and addresses. On other channels, material obtained illegally from camcorders (Lee, 2021) installed in shops and changing rooms was made available for a fee (at the time of writing this article, a Google search displayed dozens of records for the term "Korean girls Telegram").

Polish anti-vaccinationists (e.g., the Kamraci Rodacy group) form small communities on Telegram, which often overlap with groups active on other social media platforms, and the videos and narratives they share mirror the anti-vaccine messages spread in other countries. Along with the issues connected with treating the coronavirus with alternative medicines, Polish users also post other material on their channels. They distribute videos documenting natural disasters in different countries, police brutality against anti-vaccine demonstrators and appeals about the need to counter oppressive regimes forcing free people to take harmful vaccinations. The content of all the posts and videos, often reproduced in different configurations by numerous small groups, is intended to serve as an illustration of the "besieged fortress" narrative. The presented examples aim at illustrating the world at its end, and this apocalyptic message reinforces the sense of entrapment and uniqueness of users of these groups and channels. Much of the material contains obvious disinformation, usually taken from German-speaking channels, with some content clearly relating to the narrative of the QAnon groups.

While the above examples prove Telegram's usefulness for various groups and non-state actors, this instant messaging platform may also, at some point in the future, make the rules of posting content more stringent. This is likely to happen given the increasing criticism in the global media or lawsuits brought against Google and Apple demanding that the app be removed from their app stores due to violent and extremist content which it is used to disseminate (Dormehl, 2021). However, financial factors may prove decisive. Expected profits among the holders of bonds issued by Mr Durov in March 2021 and a growing number of advertisers may force the owner of the app to place some restrictions on undesirable content.

Due to its wide reach, the platform is also frequently used by activists and protest organisers. In 2019, thousands of people protesting in Hong Kong against the current authorities used more than 100 groups set up on Telegram, with the aim of securing quick mobilisation and avoiding infiltration by the police. These were used to publicise information about the upcoming protests and interventions by law-and-order services, along with videos, photos and instructions for further action. In consequence, in June 2019, the platform "was subjected to a large-scale cyber-attack", as P. Durov announced, alleging that it was China that perpetrated it (Schectman, 2019).

The experience of the Hong Kong protesters was used by extensive groups of demonstrators after the presidential election in Belarus that took place in August 2020. The decision made by the authorities to decrease the speed of the country's internet resulted in an increased use of VPNs (instructions were posted on opposition Telegram channels). Lukashenka's opponents created a network of groups through which they called for protests, passed information about arrests, and published videos and photos. At the initial stage of the protests, they also publicised information from the organisers of the protests in Hong Kong, containing instructions on what to do during the demonstrations and how to use the app. These instructions mainly concerned security

issues, such as maintaining anonymity by hiding phone numbers, not giving nicknames identical to those used previously on other social networks, etc. Among many Telegram channels, Nexta TV became the most popular, enabling the posting of several hundred short films and photos each day in the initial period of the protests. In the first weeks of the demonstrations, Lukashenka officially complained that he could find no way to fight Telegram. As a result, the huge popularity of this medium forced the Belarusian authorities to adopt the communication approach used by the opposition to create their own, alternative narratives. These were, and still are, aimed at invoking fear of the omniscient authorities by publishing information about the regime's opponents and showing how brutally they are treated. For more than a year after the protests began, the Belarusian opposition and Lukashenka's regime groups and channels are active in the Russian-speaking space of the platform.

Many users believe that Telegram abstains not only from seriously interfering with posted content but also from passing on information about individuals or communication keys to any state or entity. The reality, however, seems to be slightly different. The already mentioned closing down of certain channels as a consequence of Europol's intervention is not the only example. In 2019, Hong Kong activists pointed out that the architecture of this instant messaging platform might allow China to obtain the phone numbers of protesters. Following the aforementioned attack on Telegram, the phone number sharing feature was improved (Schectman, 2019). In June 2020, Roskomnadzor, the digital surveillance authority in Russia, which had been blocking the platform since 2018, lifted restrictions regarding the use of the app in the Russian Federation. This decision was officially justified by referring to P. Durov's commitment to cooperate with Russian authorities in the fight against terrorism advertised on the platform. Nevertheless, this fact and the current widespread use of Telegram by the Russian authorities to fight the coronavirus gave rise to some speculation that the platform owner's cooperation with the Russian Federation is not limited to fighting down extremism, but Russia has in fact gained wider access to the platform than it may seem.

References:

Ayad, M. (2020) *The Propaganda Pipeline: The ISIS Fuouaris Upload Network on Facebook* (ISD), available at: https://www.isdglobal.org/wp-content/uploads/2020/07/The-Propaganda-Pipeline-1.pdf (November 30, 2021).

Chan, S. (2021) *WhatsApp Rivals See Nearly 1,200% Growth Ahead of Privacy Policy Deadline*, available at: https://sensortower.com/blog/whatsapp-signal-telegram-install-growth (November 29, 2021).

Collins, B. & Zadrozny, B. (2021) *Anti-vaccine groups changing into 'dance parties' on Facebook to avoid detection*, available at: https://www.nbcnews.com/tech/tech-news/anti-vaccine-groups-changing-dance-parties-facebook-avoid-detection-rcna1480 (November 30, 2021).

Center for Countering Digital Hate (2021) *The Anti-Vaxx Industry. How Big Tech powers and profits from anti-vaccine misinformation*, available at: https://www.counterhate.com/anti-vaxx-industry (November 29, 2021).

Davidovic, I. (2021) *Telegram misogyny: 'They wanted to tie me and my child to a horse'*, available at: https://www.bbc.com/news/technology-56801878 (November 27, 2021).

Dormehl, L. (2021) *Coalition for a Safer Web sues Apple for not giving Telegram the boot*, available at: https://www.cultofmac.com/732764/coalition-for-a-safer-web-group-sues-apple-for-not-giving-telegram-the-boot/ (November 30, 2021).

Lee, S. (2020) *South Korea's latest sex crime scandal is a blackmail ring streaming abuse on Telegram*, available at: https://qz.com/1824130/korea-shocked-by-telegram-chat-room-sexual-abuse-scandal (November 28, 2021).

Hebel, C., Hoppenstedt, M. & Rosenbach, M. (2021) *The Telegram Billionaire and His Dark Empire*, available at: https://www.spiegel.de/international/world/the-telegram-billionaire-and-his-dark-empire-a-f27cb79f-86ae-48de-bdbd-8df604d07cc8 (November 30, 2021).

Mierzyńska, A. (2021) *Są przekonani, że walczą przeciw niewolnictwu i segregacji. Antyszczepionkowcy w Polsce*, available at: https://oko.press/antyszczepionkowcy-w-polsce/ (November 29, 2021).

Pierce, D. & Kramer, A. (2021) *Here are all the Facebook Papers stories*, available at: https://www.protocol.com/facebook-papers (November 30, 2021).

Schectman, J. (2019) *Messaging app Telegram moves to protect identity of Hong Kong protesters*, available at: https://www.reuters.com/article/us-hongkong-telegram-exclusive-idUSKCN1VK2NI (November 30, 2021).

Blocking Injunctions Against Online Intermediaries: Between EU Standards and National Peculiarities

KAROL KOŚCIŃSKI

Abstract The paper describes EU standards which set out the rules of applying one of the most effective tools used for combating online piracy – namely blocking injunctions issued against various types of online intermediaries due to copyright infringements. The author analysed the rules which have been shaped in European law and the case law of the Court of Justice of the European Union (CJEU). Against this backdrop, the differences which have emerged in the process of applying injunctions in some EU Member States have been discussed. The paper also describes the specific nature of Polish circumstances in this respect, based on the judgements of Polish courts, referring directly or indirectly to injunctions issued against online intermediaries.

Keywords: • blocking injunctions • online intermediaries • infringement of copyright • internet piracy

CORRESPONDENCE ADDRESS: Karol Kościński, Attorney-at-Law, Law Office, Ul. Marcina z Wrocimowic 12E/22, 03-145 Warszawa, Poland, e-mail: karolkoscinski@tlen.pl.

https://doi.org/10.4335/2022.2.12 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 The factual and market background of blocking injunctions

One of the numerous spheres for which the emergence of the internet posed a considerable challenge was the enforcement of exclusive rights, in particular copyrights. The challenge resulted from the development and dissemination of new methods of distribution and the use of works, engaging in the process of an entire chain of new types of intermediaries – internet service providers, hosting providers, and website operators. New models of providing access to content were not only more complicated than traditional ones, but also reflected the web-like nature of the internet. As a general use technology – regardless of the spheres it has transformed – it operates on a cross-border basis, and digital use is liberated from the need to use any tangible storage medium, with substantial anonymity given to service providers, and the easy change of location from where such services are rendered. The possibilities in this respect further expanded along with the development of broadband internet, allowing the easy streaming of works, including audiovisual works.

This new ecosystem of providing access to copyrighted content revealed the limitations of the legal instruments which have previously been used for the protection of exclusive rights. In addition to the aforementioned factual circumstances, the legal status was further complicated by the introduction of legal provisions which greatly facilitated the exclusion of online intermediaries' responsibility (Articles 12-14 of the Act 18 July 2002 on the Provision of Services by Electronic Means – Journal of Laws of 2002 No. 144, Item 1204, as amended), where their services are used or directly intended for providing access to content protected by copyright.

The domestic provisions governing this sphere have their source in European law, which continue in force to this day (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ EU L 178/1 of 17.07.2000) – the E-Commerce Directive) laying down the rules applicable to the operations of online intermediaries. The provisions were drawn up over twenty years ago and set out the circumstances in which it is possible to exclude the liability of so-called passive online intermediaries, including liability arising from the infringement of copyright. The provisions of the same legal act allowed the introduction in sector-specific regulations of the legal grounds for the adoption of measures by judicial or administrative authorities with a view to resolving individual cases of law infringement and preventing their occurrence in the future. Basic EU solutions concerning copyright, including its application in the digital sphere, were adopted almost at the same time (Article 18(1) of the E-Commerce Directive). As sector-specific regulations, they introduced legal grounds to issue injunctions against online intermediaries, including blocking injunctions (Article 8(3) of the InfoSoc Directive in respect of copyright, and Article 11 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the

enforcement of intellectual property rights, further referred to as the IPRE Directive, in respect of other intellectual property rights).

Taking advantage of unexpected interference of the two groups of legal norms, some intermediaries would abuse the possibility to evade liability for the infringement of intellectual property rights on the basis of exemptions which have been established with passive online intermediaries in mind (in particular, hosting service providers), despite the fact that their services were of a different nature. To this end – in numerous court proceedings – online intermediaries claimed that they had not infringed any copyright laws because private internet users were the ones who provided access to copyrighted content, and the intermediaries' role was limited to providing online space or technical tools which were neutral in respect of such content and allowed access to all types of content. They also noted that since they were not allowed to engage in pre-screening of content, it was impossible for them to distinguish between copyright-protected content and any content which was not subject to copyright prior to providing access to such content.

Moreover, it soon became clear that from economic, legal and political perspectives, it was pointless to prosecute private web users who illegally provided access to protected content. The costs significantly exceeded possible compensation in this case. And it was often impossible to obtain the personal data of natural persons, and the social reception of legal actions which were directed against private internet users was clearly negative.

The weaknesses of the copyright protection instruments at the time were related to the rules of tort liability (Article 415 et seq. of the Act of 23 April 1964 - the Civil Code consolidated text, Journal of Laws of 2021, Item 1509, further referred to as "the Civil Code"), which is conditional upon proof that the infringer has been actively involved in the infringement and is at fault. They require the application of the same criteria as in the case of accessories to a prohibited act (Article 422 of the Civil Code), which, in the context of the infringement of exclusive rights, in theory could be a construct capacious enough to cover the relationship between online intermediaries and private users of their services.

In such circumstances, the response of those with the right to claim the infringement of exclusive rights was usually significantly belated, at times depending on the engagement of law-enforcement authorities and the application of penal law norms, or ineffective administrative procedures (with French HANOPI being the best example here), and sometimes simply impossible. This meant that the owners of copyrights to work with the highest economic value were particularly exposed to considerable losses at the initial stage right after providing public access to them, in particular audiovisual works, TV shows, and, to a smaller extent, pieces of music and textual works. It is not a coincidence that the representatives of this group of rightsholders have begun to request injunctions against online intermediaries whose services are used by a third party to infringe exclusive

rights. (Husovec, 2017: 3 – 5). Such injunctions, including blocking injunctions which are special types of this instrument, allowed the reduction of the illegal use of specified content after a short time of their providing access to it. That way, they mitigated the financial loss incurred by rightsholders, where full compensation might not be attainable, may be limited, or where the granting of compensation might be considerably postponed.

2 The main purpose of blocking injunctions against online intermediaries, their types and the grounds for their introduction in European law

The evolution of this seemingly inconspicuous instrument which, unlike Western European countries and a dozen or so of the most developed non-European countries (the USA, Australia, Argentina, India, Indonesia, Singapore, Malaysia, South Korea, and Turkey), is not widely used in the states of our region, would surely surprise the authors of the European regulation which constitutes the grounds for its introduction across the EU. The source of said surprise would be, for instance, the laconic nature of the provisions under which EU Member States are only obligated to create the possibility to apply for the issue of the injunction. The provisions do not define the range, the content, the conditions for granting the injunction, the group of addressees or – which seemed obvious back in 2001 – any procedural issues related to the cross-border enforcement of the injunctions. EU legislators made the pragmatic assumption that online intermediaries, in many cases, simply had the real technical capabilities to effectively, and at relatively low cost, bring the infringement of exclusive rights to an end. In fact, the measures directed against them were not even referred to as sanctions but cooperation instruments (Recital 59 of the InfoSoc Directive).

In 2001, when business models for providing access to content on the internet began to evolve, few could predict what type of detailed solutions would be created on the basis of such a general norm. After ten years, or just over, it became clear that blocking injunctions represented one of the most effective and most frequently used measures, also outside of the EU, placing obligations on online intermediaries to implement technical measures to block access to specific content or websites. There is no legal definition of blocking injunctions in legal acts (Riis, Elholm, Nordberg, 2018: 5 -8).

The evolution of this legal measure led to the development of three types of injunctions, which are now applied in practice in various situations. The first type is a static blocking injunction, mostly used for websites which were created to provide access to content protected by exclusive rights. An entity which starts such a website is either not interested in cooperation with rightsholders, or has not been identified by them. In such an event, the addressee of such an injunction is not the operator of the pirate service concerned, but an internet service provider, and the result is blocked access to a specific website.

The second type is a dynamic blocking injunction which serves to facilitate the resolution of cases where content which has been shared in violation of exclusive rights on one

website appears again on another website. The outcome of such an injunction is the blocking of access to a website which might have another IP or URL address, but serves the purpose of sharing the same content as the previous one. The website is often related to its predecessor through a domain name, to ensure higher visibility and for the convenience of the users of the content who find it easier to search for a given website in a browser. A dynamic injunction must be formulated in a way which allows the rightsholders to add a new IP or URL address without the need to institute new court proceedings to obtain a new injunction. Alternatively, if given domain names and/or IP addresses are unknown to a court at the date of issuing a ruling, the courts define only the time frame (as a given period of time or until a specified date) for the rightsholders to submit to service providers a list of websites which are to be blocked on the basis of a given injunction. This way, a rightsholder does not have to apply for separate injunctions each time given protected content appears on other websites, thus allowing the reduction of costs and other inconveniences related to the proceedings. In effect, the system of exclusive rights' protection regains the necessary balance, which is only disturbed where the protection of rights is costly and long-lasting, and the breach itself, involving merely the creation of a new website and the provision of illegal access to the same content, is easy and inexpensive.

The third type is a live blocking injunction applied in real time in respect of content that is provided live. Such an injunction was used in the United Kingdom for the first time in a matter concerning the broadcasting of football matches (The Football Association Premier League Ltd. vs. British Telecommunications Plc & Others [2017] EWHC,480 (Ch). The use of such an injunction serves its purposes only during transmission, and the response of rightsholders and legal protection authorities must be swift and strictly limited in time. The technical measures indicated in the injunction are only applied each time a given server is used to provide access to a live broadcast. This means that the injunction is granted only for a strictly defined time frame, of which the rightsholder is obliged to inform the online intermediary in advance (for example by way of an electronic message from the rightsholder concerned or a third party authorised to act on the rightsholder's behalf).

Not all types of blocking injunctions are awarded, even in those Member States which introduced the general legal grounds for applying for the issue of such instruments. The possibility of applying blocking injunctions – whatever their type – was confirmed in the case law of Austria, Belgium, France, Finland, Greece, Ireland, the Netherlands, Portugal, Spain, Sweden, the United Kingdom, and Norway. In Germany and Lithuania, decrees granting blocking injunctions can be appealed against. In some jurisdictions, the option to apply dynamic injunctions or injunctions in respect of live broadcasts has not been examined by courts yet. It was attempted on several occasions but with negative effects. Case law pointed to the need to specify in greater detail the national legal grounds for applying injunctions in a situation where a simple transposition of EU law has proven to be insufficient.

Regardless of the type of injunction a rightsholder applies for in given circumstances, from a technical point of view, in practice they entail the blocking of a domain or a specific website, or the blocking of data transferred by an internet service provider. An private user's computer is then unable to locate a specific domain or website (blocking of DNS, URL or IP number), which in consequence leads to the blocked transmission of, e.g., work protected by copyright, or to the refusal of access to an entire website through which the specified content has been shared. Consequently, the content in question is not removed at source, which solves the problem of insufficient legal instruments to eliminate pirate websites operating in territories in which copyright is not protected at all, or the protection is only illusory. Any such content is simply made unavailable to recipients in the place of destination by the operator of a given pirate website. Injunctions are usually issued against several major internet service providers operating in the territory of a given Member State – if this is the case, the scale of infringement elimination is the most noticeable.

The aforementioned flexibility of EU laws might prove to be an advantage at times, as it does not exclude the possibility to use other technological measures other than the ones generally applied in blocking injunctions, allowing rightsholders and courts to adapt to changing infringement methods. On that basis, the French Supreme Court (judgement of 6 July 2017 SFR et al. vs the Association of Film Producers, No 16-17.217, 16-18.298, 16-18.348, 16-18.595, ECLI:FR:CCASS:2017:C100909) upheld injunctions under which search engines were required to de-index and block access to websites whose structures had been designed to infringe exclusive rights.

3 Standards for applying blocking injunctions in the case law of CJEU

Regardless of its potential advantages, the general wording of Article 8(3) of the InfoSoc Directive resulted in the fact that the practical application of the injunctions in individual Member States was, to a large extent, shaped on the basis of the case law of national courts and its verification by CJEU. All the more so due to the fact that in many cases the legislators who implemented EU provisions into domestic legal systems, before checking how injunctions against intermediaries could be used in practice, simply and directly rewrote this general EU legal provision in national legal acts.

Courts developed standards for applying the injunctions at the intersection of the interpretation of vague EU law provisions, setting out the criteria in which the measures for the protection of intellectual property rights must meet (e.g., they must be effective, fair and equitable – Article 3(1) of the IPRED Directive, they must be dissuasive, cannot be unnecessarily complicated or costly, or entail unwarranted delays, and should provide for safeguards against their abuse – Article 3(2) of the IPRED Directive), and of the fundamental rights stipulated in Treaties. As regards the latter provisions, the aim was to balance the interests of rightsholders, intermediaries and users in the circumstances of an

imminent conflict between the protection of ownership rights, including intellectual property rights (Article 17(2) of the Charter of Fundamental Rights of the European Union of 7 June 2016, OJ EU C 202/391, further referred to as the Charter of Fundamental Rights), the right of access to information (Article 11 of the Charter of Fundamental Rights), and the freedom to conduct business (Article 16 of the Charter of Fundamental Rights). Users' rights might be infringed if, for instance, the authorities issue blocking injunctions whose objective scope or duration is excessive, and which impose obligations that are impossible to fulfil, or injunctions concerning content which should not be blocked at all (over-blocking). In consequence, as regards renewals or the extension of such injunctions, some national courts require the prior assessment of injunction effectiveness and an examination of whether the extension of the term is appropriate (Cf. The Football Association Premier league Ltd vs. Eircom Ltd (Trading as Eir) & Others (Approved) [2020])

The final outcome of CJEU's activities is a catalogue of standards which allows the assessment of individual cases of injunctions, and some of them can be applied to all measures of this type, while others are of special significance where blocking injunctions are applied. All these standards are addressed mostly to judicial authorities, as they decide what actions, if any, the addressee of the injunctions will be obligated to take.

CJEU case law, which was partly recapitulated in the most recent Communication of the European Commission on the enforcement of intellectual property rights (Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights; COM (2017) 708 final):

- specified the term "intermediary – injunction addressee"
- indicated that the injunction applies regardless of any potential liability of the intermediary for the infringement of exclusive rights, including fault;
- specified the purpose of injunctions;
- specified in detail the circumstances which should be taken into account in the assessment of whether the issued injunction is proportional;
- indicated how courts should balance the interests of rightsholders, intermediaries and users.

The notion of an intermediary against which an injunction can be issued should be understood comprehensively. It may be any economic operator providing a service which can be used by at least one person to infringe exclusive rights (CJEU judgement in the case of L'Oréal v. eBay (C-324/09), Par. 131; C-70/10; similarly, CJEU judgement in the SABAM case – 360/10, Par. 29). This way the list of potential intermediaries remains open-ended, and it is not necessary for the infringer and the intermediary to maintain a specific relationship (CJEU judgement in the case of Tommy Hilfiger Licensing LLC et al. v. DELTA CENTER - C-494/15 paragraph 23). The CJEU also expressly confirmed

that intermediaries include internet service providers who are the most typical addressees of blocking injunctions. From an evidence-based perspective, the fact whether private users of addressees' services have actually gained access to protected content is outside the scope of proof. It is enough to demonstrate that such content is available.

As no form of intermediary's participation in infringement is required, rightsholders are not obliged to prove the intermediary's fault to obtain an injunction. In this situation, it is enough for the intermediary to provide services which might potentially be used for infringement, even if no such circumstances have occurred yet (Husovec, 2017: 132). Consequently, this also means that the intermediary cannot rely on one of the grounds for exemption of liability, as they are intended for the exclusion of fault, which is entirely beyond the scope of examination when issuing an injunction. Despite other possible interpretations (the Opinion of the Advocate General, M. Szpunar, in the Stichting Brein case (C-527/15), such solutions resulted in the fact that blocking injunctions became a convenient legal remedy from a court procedure perspective. The issue of involvement, or lack thereof, on the part of an injunction addressee, in the infringement of exclusive rights might be of key significance for the assessment of whether the obligations imposed under the injunction are excessively burdensome or costly (Piech, 2019: 337). The greater the intermediary's involvement, the more difficult it is for them to claim that the injunction constitutes a significant burden to them.

This is consistent with the purpose of the injunction, as broadly described in the case law of the CJEU. The purpose is not only to resolve existing infringements, but also to prevent future infringements involving the illegal use of copyrights; this way, blocking injunctions also play a preventive function (CJEU judgement in the case of Tobias Mc Fadden v. Sony Music Entertainment Germany Gmbh (C-484/14); similarly in the aforementioned judgement in the case of L'Oreal v. Ebay (C-324/09)). In practice, such objectives of an injunction have opened the door to the application of dynamic blocking injunctions. Furthermore, with the further evolution of case law, it has allowed the determination of whether it is possible to block identical or equivalent websites of different IP or URL addresses, instead of a more restricted obligation to apply specified technical measures to block a specific IP or URL address. It is important to assume here that an equivalent website is one whose content remain essentially unchanged or diverge very little from the content which had resulted in identifying the original infringement (Cf. CJEU judgement in the case of Eva Glawischnig-Piesczek v. Facebook Ireland Ltd (C-18/18) which applies to the protection of personal interests, but also has implications for intellectual property rights).

On assessing which blocking injunctions are proportional, first and foremost it is important to analyse whether the measures arising from a specific injunction are possible for the intermediary concerned to undertake in practice. Here, the first group of circumstances entails the organisational and financial capabilities of the injunction addressee, including those related to potential complaints from consumers which may be

filed if the blocking of specific content proves to be unfounded. Potentially contested issues might also include the situation in which costs are imposed only on the intermediary (CJEU judgement in cases Scarlet v. Sabam (C-70/10) and Scarlet v. Netlog (C-360/10), in particular where the intermediary itself does not infringe exclusive rights. It is a more reasonable solution to split the costs between two parties, or even have the costs incurred by the rightsholder, in particular considering that it is surely the rightsholder that draws economic benefit from enforcing the injunction.

In some cases, the distribution of the costs arising from injunctions is governed in a given EU Member State by laws concerning enforcement proceedings. The effectiveness of a given injunction is the second criterion through which its proportionality can be examined. (Cf. CJEU judgement in the Telekabel Wien case - C-314/12). It would be utopian to believe that a given injunction must be fully effective or that there is no possible way to circumvent the technical measures indicated in the injunction. It is enough to ensure that the injunction partly prevents infringements or significantly hinders such conduct. The standard of expectations towards the addressees of injunctions is connected with the obligation to take reasonable and justifiable efforts in the circumstances of a given case, to at least discourage infringement. Consequently, an injunction which, in given circumstances, is completely ineffective or requires unacceptable efforts on the part of the addressees, cannot be issued.

It is clear that the criteria taken into consideration in the context of blocking injunctions for the assessment of fundamental rights are mostly open-ended. In fact, it is criticised by some legal commentators as an expression of the excessive discretion left to the judge who makes a ruling in a given case (Husovec, 2017: 190). As regards the right to information, a significant boundary is marked out here by the prohibition to issue injunctions which would not serve their purpose while unreasonably depriving users of legitimate access to given content. In practice, it was found to be acceptable to block access to a given website if only some of the works available there have been shared illegally, with other content being considered legal. The laws of individual EU Member States usually provide private users with the possibility to file a complaint against the actions of intermediaries who have infringed a users' right to information when fulfilling obligations imposed on it under an injunction. Users may also request a judicial authority to withdraw or amend blocking injunctions. In practice, users seldom turn to these type of measures. One of the reasons might be the insubstantiability of such complaints where it is clear that the blocked website was designed to infringe exclusive rights. Another factor includes the costs of such proceedings which might simply discourage private users. Leaving aside the issue of exercising remedies by private users in practice, there is no doubt that their interests may be give due regard both at the stage of issuing injunctions and thereafter. As regards the protection of the freedom to conduct business, as a rule, it was assumed that blocking injunctions are without prejudice to its essence if they are clearly specified (Piech, 2019: 356). Besides, the intermediary itself can reduce the costs

it has incurred by adopting reasonable measures to meet its obligations (Shapiro, 2019: 29).

4 Key similarities and differences between EU Member States in their application of blocking injunctions

The standards governing blocking injunctions which arise from CJEU case law impose certain evidence-related obligations on entities seeking to protect their rights through this measure.

As a rule, the obligations are similar in every jurisdiction, but due to, for instance, the differences in procedural laws, they may be fulfilled in various ways. To some extent, they arise from the essence of the injunction itself – as a targeted legal measure, related to a strictly defined online intermediary, and individualised, at least to some degree, websites or content. Its application must be limited in time; it is another manifestation of the targeted nature of the injunction which constitutes a kind of security against disproportionate measures, at the same time imposing additional obligations related to the proceedings.

In the course of an injunction procedure, the rightsholder should precisely indicate the service which is used for the infringement of exclusive rights and the addressee of the injunction, namely the entity providing such a service. In addition, the applicant must present evidence showing they are entitled to intellectual property rights which are to be protected, and circumstances confirming the infringement itself or the possibility of its occurrence. No special rules as regards evidence have been provided in the course of this procedure – applicants mostly use screen shots, various types of technical reports or testimonies, but also notifications of recurring infringements which have been sent to future injunction addressees prior to applying for this legal measure. As confirmed multiple times by courts in Member States, there is no reason to provide evidence showing the type of the intermediary concerned (access provider versus content provider) or the degree of its engagement in the process of copyright infringement (Cf. Court of Milan, Ordinance No. 42163/2019 R.G. of 5 October 2020, Sky Italia, Lega Serie A v. Cloudflare et al.).

Blocking injunctions issued by national courts usually apply to internet access providers under the jurisdiction of a relevant Member State and to illegal actions having consequences in the same territory. Courts may order the blocking of illegal content regardless of the place where the infringement of Intellectual property rights has taken place or the location where users having access to the content stay, unless the illegal actions are addressed to users in a given Member State. Injunctions are legal instruments with a specified territorial scope, which corresponds to the territorial nature of copyright protection, and at the same time, as already noted, solve the problem of their protection, omitting the resulting limitations. The procedures for the issue of injunctions are currently

conducted in each EU Member State in line with national procedural laws. An additional source of divergence in this respect may also come from the method of transposing European legal provisions to national legal systems, as not all countries did this by simply rewriting specific European laws to national regulations.

In this case, the consequences are burdensome to rightsholders. Even if all such actions refer to the same intermediary, the same protected content and the same period of use, it is necessary to conduct separate procedures in each jurisdiction. From the perspective of rightsholders, this requires them to coordinate their legal actions if, at the same time (e.g., during a film première), an injunction is to exert real influence across a larger territory than the one delimited by the boundaries of one EU Member State. The systemic consequence is the lack of cross-border enforcement of injunctions. Perhaps the introduction of new rules as part of the so called Digital Service Act will change this state of affairs (Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services – COM(2020)825 in a version proposed by the European Commission, further referred to as the Draft DSA Regulation) The Draft sets out the minimum conditions an injunction should meet to be enforced in a Member State other than the issuing country (Article 8 of the Draft DSA Regulation) and establishes a network of Digital Services Coordinators who are to facilitate the cross-border enforcement of legal protection measures on the internet, including blocking injunctions (Article 38 of the Draft DSA Regulation).

In addition to the issue of cross-border enforcement of injunctions, other procedural differences include:

- the scope of determining the circumstances of a case;
- the participation of both parties in proceedings aimed at issuing injunctions;
- the possibility for an online intermediary to suspend the application of a relevant injunction;
- the scope of remedies available to users and online intermediaries.

In the first case, if an injunction is to be permanent, it is necessary to examine all circumstances of infringement to assess the facts in terms of general rules formulated in the case law of the Court of Justice of the European Union. In cases of interim injunctions in urgent matters, the courts are equipped with a broader scope of judicial freedom; they can rely on prima facie evidence of certain circumstances to a greater extent (Mapping report on the national remedies against online piracy of sports content, 2022: 80).

In the second case, in some countries (Greece, Ireland, and Spain) procedural laws stipulate mandatory participation of all the parties involved in proceedings aimed at issuing injunctions. However, in some Member States, ex-parte proceedings are possible under certain conditions. The conditions include an urgent need to issue an injunction (Germany), a situation where the infringement of exclusive right has already occurred (the Netherlands), or the online intermediary concerned has been previously informed

about infringements / the rightsholders' intention to resort to an injunction (the United Kingdom).

In turn, the suspension of injunctions, which is not a European standard, but has been developed under the case law in Ireland and the United Kingdom, is of a temporary nature. Suspension or blocking may be requested in order to correct or investigate the possible over-blocking of material, to maintain the uninterrupted operation of the service provided by the intermediary concerned or from a technical point of view (e.g., to preserve the integrity of the service, for maintenance or removal of direct threats to the security of the network, service or the intermediary).

As regards the fourth point, the laws of all EU Member States provide for remedies which allow addressees to contest blocking injunctions in line with traditional rules of civil procedure. Remedies are available to intermediaries and alleged infringers affected by an injunction. In addition, several Member States have the right to remedies vested in private internet users affected indirectly by a given injunction (e.g., in Finland, Germany, Greece, Ireland, the Netherlands, and in the United Kingdom). According to the German Supreme Court (Frosio, 2021:627), private internet users have the right to a legal remedy by starting an action against their access provider on the basis of their contractual relationship. Moreover, in a few cases (the Netherlands), class actions by internet users against blocking injunctions are available, or internet users' rights are protected under consumer protection laws.

In addition to the issues related to court proceedings, significant differences between EU Member States in respect of blocking injunctions are related to the possibility of their issue by administrative authorities (such options can be exercised in Greece, Italy, Spain and Lithuania), or to the facilitating of their enforcement through self-regulatory solutions (for instance, in Belgium, joint contact points have been established by the rightsholders and the potential addressees of blocking injunctions with a view to receiving and examining complaints, i.a., against the infringement of exclusive rights). As regards the former solution, the relationship between proceedings conducted before administrative and judicial authorities may vary: usually, both measures are not mutually exclusive, although there are instances where the institution of an administrative procedure excludes the possibility to bring civil action. In the latter case, these are solutions of limited scope and applicability, which are only intended to facilitate protection, supplementing official proceedings or ensuring appropriate solutions before formal procedures are instituted.

5 No grounds for applying blocking injunctions in Polish law

Apart from Lithuania, blocking injunctions are not used in EU Member States in our region. As confirmed by one of the few rulings that discuss the issue, there is no specific legal basis which would allow for such injunctions to be requested at courts (Cf. judgement of the Court of Appeal in Warsaw in the case of Wolters Kluwer Polska S.A.

v. FS File Solutions Limited based in Nicosia (Cyprus) – Case file No. ACz 164/17). In the discussed ruling, the court found that preventive measures imposed by judicial authorities may only refer to a specified infringement of copyright, and should not expand to multiple infringements, even in respect of the same right, infringements which occur at the same moment or might occur in the future. Furthermore, the court has pointed to the fact that specified infringement means an infringement which was made or which can be made by a specific infringer, not the existence of an abstract threat related solely to the business profile of a given online intermediary. Thus, the court decided that it was not possible to impose a general or abstract injunction which would cover all audio-visual work, even if they are the property of a given rightsholder.

The absence of a proper provision allowing the issue of blocking injunctions – similarly as in several other EU countries – is subject to a complaint submitted with the European Commission by rightsholders concerning the failure to implement European law in the domestic system, which has not resulted in the institution of a formal procedure in this respect so far.

In such circumstances the only provision which would be used for obtaining similar, though limited in effect in respect of copyright, is Article 79(1)(2) of the Act of 4 February 1994 on Copyright and Related Rights, stipulating that a claim for remedying infringement may be filed. The enforcement of such claims may consist in, i.a., the removal of content shared by infringing exclusive rights. It is worth mentioning here the decision of the Court of Appeal in Kraków of 18 September 2017 (Case file No. I Ca 1494/15), in which the court ordered internet service providers to delete a user's account with a link to illegal content. In the statement of reasons, the court found that online intermediaries were not passive as they charged fees for the downloading of content, thus attributing fault to these entities for the infringement of exclusive rights. Therefore, the court focused on the intermediary's participation, and consequently on the liability for infringement, and not on the possibility to impose a specific obligation aimed at protecting rights, regardless of such participation and fault on the part of the intermediary. Yet this is the essence of blocking injunctions. It is worth stressing that this single instance of a ruling does not confirm that the possibility to issue blocking injunctions exists in Poland. Rather, it constitutes an attempt to propose a temporary substitute measure of limited scope of application in anticipation of necessary legislative intervention.

6 Conclusions

1. In Polish law, there are no grounds for courts to apply injunctions against online intermediaries which are not directly involved in copyright infringement. This means that full compliance of Polish copyright laws with European regulations (Article 8(3) of the InfoSoc Directive) has not been provided. Due to the planned entry into force of the DSA Regulation and the resulting need to indicate the authority responsible for the fulfilment of obligations related to the cross-border enforcement of injunctions against online

intermediaries, the implementation of European legal norms governing blocking injunctions is even more important. It is difficult to substantiate a situation where Polish judicial authorities will be obliged to enforce injunctions protecting the rights vested in rightsholders from other EU Member States, and, at the same time, Polish rightsholders will be deprived of the possibility to use such a protective measure, both in Poland and across the EU.

2. Some courts try to fill this gap by applying provisions that allow for the exclusion of liability for online intermediaries', in line with their original scope, solely in respect of passive intermediaries, which results in imposing specific obligations on intermediaries. However, this solution does not provide rightsholders with effective and expedient tools for limiting the scale of internet piracy, and requires a complex investigative procedure. In addition, court rulings in this respect are scarce, and it is difficult to speak about any case-law practice here.

3. Relying on the experience of more advanced EU Member States, Polish legislators should introduce to the Copyright Act a legal basis creating the possibility for courts to issue blocking injunctions against online intermediaries. Such legal regulations should take into account the standards developed by CJEU case law which were partly confirmed in the Communication of the European Commission on the enforcement of intellectual property rights. The most important elements to consider here include:

- developing a comprehensive group of injunction addressees;
- making the possibility to issue an injunction no longer contingent on the intermediary's participation in respect of the infringement of copyright
- the determination that courts are authorised to issue dynamic injunctions and orders addressed to live streaming websites.

Given the solutions included in the Draft DSA Regulation, it is also advisable to define the minimum elements of an injunction in a way consistent with the Regulation to assure the possibility of the cross-border enforcement of injunctions issued by Polish courts.

4. Taking into consideration the negative experience of some EU Member States with overly laconic laws governing the issue of injunctions against online intermediaries, and potential public debate on the laws aimed to block access to internet content, the proposed Regulation should include provisions which clearly define available remedies as part of the appeals procedure. Legislators should also provide the possibility to apply for suspending an injunction, if it has ceased to perform its function, if such need arises from technical circumstances or changed facts related to the operations of a given intermediary and results in the over-blocking of content.

5. The laws should also specify the rules for splitting the costs of blocking injunctions, at least in the situation where an injunction is issued against an intermediary which is by no means engaged in the infringement of copyright (i.e., access providers). Imposing

injunction enforcement costs exclusively on intermediaries is not justifiable from the perspective of equity rules, and will not contribute to the development of long-lasting relationships between rightsholders and online intermediaries.

References:

Frosio, G. (2021) Enforcement of European Rights on a Global Scale, In: Rosati, E. (ed.) *The Routledge Handbook of European Copyright Law* (London: Routledge), pp. 613-641.

Frosio, G. & Bulayenko, O. (2021) *Study on dynamic blocking injunctions in the European Union* (Alicante: European Union Intellectual Property Office).

Husovec, M. (2017) *Injunctions against intermediaries in the European Union. Accountable but not Liable?* (Cambridge: Cambridge University Press).

European Audiovisual Observatory (2022) *Mapping report on the national remedies against online piracy of sports content* (Strasbourg: European Audiovisual Observatory).

Piech, M. (2019) *Pośrednicy internetowi w prawie Unii Europejskiej* (Warsaw: Wolters Kluwer).

Riis, T., Elholm, T. & Nordberg, A. (2018) *Study on Legislative Measures Related to Online IPR Infringements* (Alicante: The European Union Intellectual Property Office).

Swiss Institute of Comparative Law (2015) *Filtering, blocking and the take-down of illegal content on the Internet* (Lausanne: Council of Europe).

Shapiro, T. (2019) Directive 2001/29/EC on copyright in the information society, In: Shapiro, T. & Lindner, B. (ed.) *Copyright in the Information Society: A Guide to National Implementation of the European Directive* (London: Edward Elgar Publishing), pp. 40 -125.

Solutions on Blocking Access to and Removing Illegal Content on the Internet Under EU Regulations and Polish Law

FILIP RADONIEWICZ

Abstract The aim of this study is to present EU regulations aimed at tackling illegal content on the internet by blocking or removing it, as well as the state of their implementation into the Polish legal system. Accordingly, the first part describes the provisions of the Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, Directive 2017/541 of 15 March 2017 on Counteracting Terrorism, Regulation 2021/784 of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online (TERREG) and Directive 2019/790 of 17 April 2019 on Copyright and Related Rights in the Digital Single Market. The second part confronts them with Polish solutions addressing the subject of blocking and removing illegal content, as provided for in the Code of Criminal Procedure, the Act on the Internal Security Agency and on the Intelligence Agency of 24 May 2002 and the Act on Gambling Games of 19 November 2009.

Keywords: • blocking website access • terrorism • pornography • intellectual property • digital market • gambling

CORRESPONDENCE ADDRESS: Filip Radoniewicz, Ph.D., Expert, War Studies University in Warsaw, Academic Centre for Cyber Security Policy, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: filip.radoniewicz@radoniewicz.eu, ORCID: 0000-0002-7917-4059.

https://doi.org/10.4335/2022.2.13 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

European Union legislation provides that two categories of illegal content on the internet, due to its significant social noxiousness, should be tackled (i.e., blocked or removed) in an institutionalised manner, directly by state authorities. These are, of course, child pornography and so-called terrorist content.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and replacing Council Framework Decision 2004/68/JHA (Official Journal EU L 335, 17.12.2011, p. 1) requires Member States to take measures to remove websites containing or disseminating child pornography hosted in their territory and to take steps aimed at ensuring the removal of such websites hosted outside of their territory. Under Article 2(a) any person below the age of eighteen years is a child. However, "child pornography" means (Article 2(c)):

(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;
(ii) any depiction of the sexual organs of a child for primarily sexual purposes;
(iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or
(iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes.

Furthermore, Article 25(2) of Directive 2011/93/EU allows Member States to take measures to block access to websites containing or disseminating child pornography towards on the internet within their territory, stipulating that such measures must be set following transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate to the intended purpose; the regulation is to require state authorities to inform users of the reason for any restriction. Those safeguards shall also include the possibility of judicial redress (Article 25(2)). The provisions of the Directive on safeguards refer only to measures aimed at blocking access to websites. However, in the light of Recital 47, they should refer to both the blocking and the removal of websites.

Directive 2017/541/EU of the European Parliament and of the Council of the 15th March 2017 on Combating Terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Official Journal EU L 88, 31.3.2017, p.6) contains provisions similar to those of Directive 2011/93 with regard to "online content" constituting a public provocation to commit a terrorist offence.

Pursuant to Article 3(1) and (2) of Directive 2017/541, a terrorist offence means intentional acts defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, and which meet two conditions. First, they are listed in the catalogue contained in Article 3(1) (e.g. attacks

upon a person's life which may cause death, attacks upon the physical integrity of a person, kidnapping or hostage-taking). Secondly, they were committed with one of the aims listed in Article 3(2):

(a) seriously intimidating a population;
(b) unduly compelling a government or an international organisation to perform or abstain from performing any act;
(c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

Member States are required to develop regulations to ensure the prompt removal of "terrorist content" hosted in their territory, obliging them to take measures and actions to ensure that such content hosted outside their territory is removed. It also provides, similarly to Directive 2011/93, that Member States may, when removal of the content constituting a public provocation to commit a terrorist offence at its source is not feasible, take measures to block access to such content towards internet users within their territory. Removal and blocking measures must be set following transparent procedures and provide adequate safeguards, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress.

The EU legislators considered the requirement for Member States to regulate the subject of making terrorist content available on the internet by means of Directive 2017/541 to be insufficient, since, even during the period of its implementation (its provisions had to be transposed into national law by 8 September 2018), work was initiated on a regulation intended to regulate only this matter.

As stated in the Explanatory Memorandum of the Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online (the so-called TERREG – from terrorism and regulation), although hosting service providers, responding to calls from public authorities, have put in place certain measures to tackle terrorist content on their services (progress has been made through voluntary frameworks and partnerships including the EU Internet Forum which was launched in December 2015 under the European Agenda on Security promoting Member States' and hosting service providers' voluntary cooperation and actions to reduce accessibility to terrorist content online), they are not sufficient. However, there is – in the Commission's view – a clear need to intensify the European Union's measures against terrorist content online. On 1 March 2018 the Commission adopted – based on Communication from the Commission of 28 September 2017 on Tackling Illegal Content Online and towards the enhanced responsibility of online platforms – a recommendation on the effective fight against illegal content online. The Commission, indicating series terrorist attacks in the EU and the fact that terrorist content is still easily accessible, found it necessary to establish a clear and harmonised legal framework for the purpose of

preventing and addressing the dissemination of terrorist content online, and that the best way to do this would be to issue a Regulation. This proposal was prepared as a contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 (Radoniewicz, 2021: 164-65).

In the light of Article 1(2) of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online (TERREG), its provisions apply to hosting service providers offering services to the society in the Union, irrespective of where their main establishment may be placed.

In the light of Article 2(1) of the Regulation, the term "hosting service provider" means a provider of Information Society services involving the storage of information provided by, and at the request of, a content provider, as well as making the information stored available to the public. This applies only to services provided to the public within the application layer. Providers of cloud infrastructure services and providers of cloud services are not considered as hosting service providers. In addition, the Regulation will not apply to electronic communications services as referred to in Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Official Journal EU L 321, 17.12.2018, p. 36), i.e. services normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, with the following types of services:

a) "internet access service" as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
b) "interpersonal communications service"; and
c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.

"Content provider" means a user that has provided information that is, or that has been, stored and disseminated to the public by a hosting service provider.

"Terrorist content" means material belonging to at least one of the following categories, identified by their purpose, which is:

a) inciting the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such attitudes of soliciting, directly or indirectly, for instance through the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing danger that one or more such offences may be committed;
b) soliciting a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU)

2017/541, thereby causing danger that one or more such offences may be committed;

c) soliciting a person or a group of persons to participate in the activities of a terrorist group, including through delivery of information or material resources, or by financing the activities of that group in any other way within the meaning of point (b) of Article 4 of Directive (EU) 2017/541; thereby causing danger that one or more such offences may be committed;
d) providing instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;
e) posing a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, thereby causing danger that one or more such offences may be committed;

"Dissemination to the public" means the making available of information, at the request of a content provider, to a potentially unlimited number of persons. "Competent authority" shall mean a single judicial or independent administrative authority designated in a Member State for the purposes listed in Article 12(1) of the Regulation, i.e. :

a) issuing removal orders pursuant to Article 3;
b) scrutinising removal orders pursuant to Article 4;
c) overseeing the implementation of specific measures pursuant to Article 5;
d) imposing penalties pursuant to Article 18.

The Regulation provides that the competent authority of each Member State shall have the power to issue a removal order requiring hosting service providers to remove terrorist content or to disable access to terrorist content in all Member States (Article 3(1)).

Where a competent authority has not previously ordered a hosting service provider to remove content, it shall contact that hosting service provider, providing it with information on the applicable procedures and deadlines, at least twelve hours before issuing the removal order. Hosting service providers shall remove terrorist content or disable access to terrorist content as soon as possible and in any event within one hour of receipt of the removal order.

Where the hosting service provider does not have its main establishment or legal representative, that authority shall submit a copy of the removal order to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative is established.

A hosting service provider may take specific measures to protect its services against the dissemination to the public of terrorist content. (Article 5(2)).

Under Article 6(1), hosting service providers shall preserve terrorist content which has been removed or access to which has been disabled as a result of a removal order, or of specific measures pursuant to Article 3 or 5, as well as any related data removed as a consequence of the removal of such terrorist content, which are necessary for:

1) administrative or judicial review proceedings or complaint-handling under Article 10
2) the prevention, detection, investigation and prosecution of terrorist offences.

Article 18 requires Member States to establish penalties (since the general term "penalties" is used, this means that they can be of any nature: legal, administrative or civil, in this case they are both administrative and legal) applicable to infringements of the Regulation by hosting providers and to take all measures necessary to ensure that they are implemented. Member States shall ensure that a systematic or persistent failure to comply with obligations pursuant to Article 3(3) is subject to financial penalties of up to 4% of the hosting service provider's global turnover of the preceding business year.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Official Journal EU L 130, 17.5.2019, p. 92) focuses on three fundamental issues:

- adapting certain exceptions (e.g. text and data mining for scientific research, making copies of any work or other protected subject matter for the purpose of preserving it as national heritage) to copyright and related rights to digital and cross-border environments;
- improving licensing practices and ensuring wider access to content;
- ensuring a well-functioning marketplace for copyright.

The Directive modifies eleven directives that regulate the subject of the protection of intellectual property under EU law, including in particular Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (Official Journal EC 2001 L 167/10) and Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights (Official Journal EU 2004 L 157/45).

It aims to facilitate the use of copyright-protected material for various purposes, mainly those related to access to knowledge, by introducing mandatory copyright limitations to promote text and data mining (understood as any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes patterns, trends and correlations), digital use of works for the purpose of illustration for teaching, and the preservation of cultural heritage. In addition, it aims to facilitate licensing to ensure wider access to content, to strengthen the protection of press publications in terms of online use, and – which was controversial already at the drafting

stage – to modify the rules of using copyright-protected content by online content sharing platforms. Within the meaning of the Directive, "online content-sharing service provider" means a provider of an information society service of which the main, or one of the main purposes, is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes.

Providers of services such as not-for-profit online encyclopedia's, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms, providers of electronic communications services as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, Official Journal EU 2018 L 321/36) (pursuant to Art. 2(4) of Directive 2018/1972, are electronic communications services which means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, with the following types of services: "internet access service"; "interpersonal communications service"; services consisting wholly or mainly in the conveyance of signals, online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use, are not "online content-sharing service providers" within the meaning of the Directive.

An online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users.

An online content-sharing service provider shall therefore obtain authorisation from the rightsholders referred to in Article 3(1) and (2) of Directive 2001/29/EC (i.e., authorisation for any acts of communication to the public or making available to the public), for instance by concluding a licensing agreement, in order to communicate to the public or make available to the public works or other subject matter (Article 17(1) of the Directive).

If an online content-sharing service provider has not concluded relevant licensing agreements, they may avoid liability if it proves that it:

a) made best efforts to obtain relevant authorisation from the authors (e.g., attempted to conclude a licence agreement, but for some reasons beyond their control has failed to do so),
b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided service providers with the relevant and necessary information (it has to block access to the content it does not hold rights to

– for this purpose it is necessary to employ persons browsing the uploading of material or the use of appropriate algorithms searching for the content it did not obtain authorisation for); and in any event,

c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightsholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future upload in accordance with point (b).

A consequence of the above-discussed regulation is the necessity to filter content uploaded in the service provider's resources. At this point, it is difficult to determine whether there is validity to concerns as to whether content filtering will worsen the conditions of information circulation and thus come into conflict with the fundamental human right of freedom of expression (Machała, 2019: 987, Markiewicz, 2021). It will undoubtedly cause the operating costs of service providers to increase due to the need to invest in suitable content filtering tools. In addition, the Directive requires that blocking should be reviewed by a humans – outcomes produced by algorithms are not sufficient, since the final decision whether the request is legitimate belongs to a human (this will undoubtedly increase the operating costs of entrepreneurs as they will need to hire staff to handle this task). (Radoniewicz, 2011: 173-183)

There are exemptions from the above regulation (Article 17(6) of the Directive). They apply to new online content-sharing service providers where the services of which have been available to the public in the EU for less than three years and which have an annual turnover below EUR 10 million. However, they are obliged to make best efforts to obtain relevant authorisation from the authors and to act expeditiously upon receiving a sufficiently substantiated notice, to disable access to the notified works or other subject matter or to remove those works or other subject matter from their websites. Nevertheless, where the average number of monthly unique visitors of websites hosted by such service providers exceeds five million, calculated on the basis of the previous calendar year, they shall also demonstrate that they have made best efforts to prevent further uploads of the notified works and other subject matter for which the rightsholders have provided relevant and necessary information.

Another obligation imposed by the Directive on online content-sharing service providers is to shape the cooperation with rightsholders in such a way that it does not result in the prevention of the availability of works or other subject matter uploaded by users which do not infringe copyright and related rights, including where such works or other subject matter are covered by an exception or limitation. It should not be forgotten that it is possible to use someone's copyrighted works without infringing them, and therefore without the need to obtain a licence, under:

1) the right to quote,
2) the right to criticise or review (e.g. by creating a review of a film using extracts from it),

3) the right to parody or pastiche (e.g., creating memes).

In addition, online content-sharing service providers are required to put in place an effective and expeditious complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them.

The Directive provides that where rightsholders request to have access to their specific works or other subject matter disabled, or to have those works or other subject matter removed, they shall duly justify the reasons for their requests. Complaints submitted under this mechanism shall be processed without undue delay, and decisions to disable access to or remove uploaded content – as signalised hereinabove – shall be subject to human review. The Directive puts emphasis on the out-of-court settlement of possible disputes, as long as it can be ensured that they can be resolved impartially and that the decision ruled under this procedure by a court or other judicial authority can be reviewed.

The proposal for the Directive was criticised at the stage of being drafted, mainly by internet users (who feared that the uploading of their own content would be prevented), intermediary providers (who did not agree with imposing on them additional obligations in the form of data filtering) and human rights defenders (pointing out that, according to the case law of the Court of Justice, the prohibition of general monitoring provided for in Article 15 of Directive 2000/31 is aimed at protecting not only online intermediaries, but also fundamental rights, including the right to conduct business, and above all – the freedom of speech and the right to the protection of personal data – judgement of 16 February 2012 in case C-360/10). (Radoniewicz 2021: 181-183)

As far as the Polish regulations on blocking access to websites are concerned, we should first mention the procedure involving online terrorist content. Pursuant to Article 32c of the Act on the Internal Security Agency and on the Intelligence Service of 24 May 2002 (Journal of Laws of 2020, item 27, as amended; hereinafter the ISA Act) for the purpose of preventing, counteracting and detecting terrorist offences and prosecuting their perpetrators, the Regional Court in Warsaw, at the request of the Head of the ISA, filed after obtaining the written consent of the Attorney General, may order a provider of electronic services, by way of a decision, to block (no possibility to remove has been foreseen) access to specific IT data related to a terrorist event or specific communication and information services aimed at or used to cause a terrorist event, available in the communication and information system, hereinafter referred to as "access block". The request shall be accompanied by material justifying the need to use this measure.

At the same time, the legislators have provided for an accelerated procedure. Namely, in urgent cases, where any delay could result in a terrorist event. The Head of the ISA, after obtaining the written approval of the Attorney General, may order to block access, at the same time requesting the court to issue a decision in this regard. The provider of electronic

services, which is to be required to block access, shall promptly perform the actions specified in the court's decision or the request forwarded to it by the Head of the ISA.

The access block is ordered for a period not longer than thirty days. If this period proves to be too short (the reasons for the block have not ceased), the Head of the ISA may file a request, approved by the Attorney General, for a single extension of the access block for a period not longer than three months.

The afore-said requests of the Head of the ISA shall be examined by a court with a panel of one judge. The entire procedure – the actions undertaken and their content are protected by the provisions of the Act on the Protection of Classified Information. Court actions related to the examination of these requests should be performed under the conditions envisaged for the provision, storage and disclosure of classified information and with appropriate application of the provisions issued on the basis of Article 181 § 2 of the Code of Criminal Procedure (the Act of 6 June 1997 – the Code of Criminal Procedure); i.e. the Regulation of the Minister of Justice of 9 September 2017 on the Manner of Handling Interrogation Protocols and Other Documents or Subject Matter Covered by the Obligation to Maintain the Confidentiality of Classified Information or to Keep the Secret relating to the Practise of a Profession or the Performance of a Function (Journal of Laws of 2017, item 1733). The Court, the Prosecutor General and the Head of the ISA shall keep in electronic form, in compliance with the provisions on the protection of classified information, a record of decisions, written approvals, orders and requests regarding an access block. The files should be stored in the court's secret office and made available only there. Only a prosecutor and the Head of the ISA may participate in the court session.

Court decisions on the application of the block may be appealed against pursuant to generally applicable rules with the Head of the ISA and the Prosecutor General. The appeal is governed by the relevant provisions of the Code of Criminal Procedure.

Pursuant to Article 32c (11), an access block shall cease in the following events:
1) the court’s refusal to authorise the Head of the ISA, within five days of filing the request pursuant to paragraph 4, to order an access block;
2) the court’s refusal to agree to extend the access block;
3) expiration of the period for which the access block was imposed;

if the provider of electronic services has its registered office in the territory of the Republic of Poland The Head of the ISA notifies the minister competent for the computerisation of the imposition of an access block.

It should be pointed out that the implementation of the Directive is incomplete. The judicial review for the application of an access block has been envisaged, but there is no access to the judicial route for entities affected by such a block (see Article 21(3) *in fine* of Directive 2017/541). It should be emphasised that publishing content online falls

within the scope of the freedom of speech in its broadest sense – Article 10 of the European Convention on Human Rights and Article 11 of the CFR (Matusiak-Frącczak, 2019).

Article 15f(5) of the Act of 19 November 2009 on Gambling Games (Journal of Laws of 2020, item 2094 as amended) provides for the possibility to require telecommunications undertakings providing services related to internet access to:

1) prevent access, on a free of charge basis, to websites using the names of internet domains entered in the Register of domains used to offer gambling games in violation of the Act through their removal from the communication and information systems of telecommunications undertakings, intended to change internet domain names to IP addresses, within forty-eight hours following the entry in the Register, at the latest;
2) re-route, on a free of charge basis, connections referring to the names of internet domains entered in the Register to the website maintained by the minister competent for public finance, containing a message addressed to recipients of the internet access service, comprising, in particular, information on the location of the Register, entering a searched internet domain in this Register, a list of entities legally offering gambling games in the territory of the Republic of Poland as well as notification of potential penal and fiscal liability of a participant of games arranged in violation of the Act.
3) enable access, on a free of charge basis, to websites using the names of domains deleted from the Register, within forty-eight hours following the deletion of the name of the internet domain from the Register.

The aforementioned "Register of domains intended for offering gambling games in violation of the Act" is maintained by the Minister competent for public finance in a communication and information system enabling the automatic transmission of information to communication and information systems of telecommunications undertakings and providers of payment services. Entry into the Register is undertaken for domain names which:

a) are used for arranging gambling games, or
b) serve the advertisement or promotion of gambling

- in contravention of the law, and which are available to internet users located in the territory of the Republic of Poland (see Article 15f (1-4)).

The afore-discussed regulation is not provided for in EU law. Its admissibility was explicitly stated in the Ladbrokes judgement (CJ judgement of 3 June 2010, C-258/08, Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd v Stichting de Nationale Sporttotalisator), in which the Court of Justice stated that blocking access to websites offering illegal gambling services is a natural consequence of the legislation in force, allowing gambling services to be offered by a monopolist to the exclusion of others.

Blocking access to gambling websites that are illegal in the territory of a Member State ensures legislative effectiveness (Lewandowicz, 2017: 14-21).

Article 218a of the Code of Criminal Procedure provides for blocking access to websites as a quasi-measure to secure evidence. In the light of § 1 of this article, offices, institutions and entities conducting telecommunication activities or providing electronic services and digital service providers are obliged to immediately secure, at the request of a court or prosecutor as contained in the decision, for a specified period of time, which shall not exceed ninety days, IT data stored in devices containing this data on a carrier or in an IT system. In the matters involving the offences specified in:

- Article 200b of the Penal Code (Act of 6 June 1997, Journal of Laws of 2021, item 2345, as amended, hereinafter: the PC) (promotion and praising of paedophilic behaviour),
- Article 202 § 3 of the PC (producing, recording, importing, storing or possessing for the purpose of distribution pornographic material with the participation of a minor or related to the presentation of violence or the use of an animal, or distributing or presenting such material),
- Article 202 § 4 of the PC (recording pornographic material with the participation of a minor),
- Article 202 § 4a of the PC (storing, possessing or gaining access to pornographic material with the participation of a minor),
- Article 202 § 4b of the PC (production, dissemination, presentation, storage or the possession of pornographic material presenting a produced or processed image of a minor participating in sexual activity),
- Article 255a of the PC (dissemination of content likely to facilitate the commission of a terrorist offence),
- Chapter 7 of the Act of 29 July 2005 on Counteracting Drug Addiction (Journal of Laws of 2020, item 2050, as amended),

a security may involve the obligation to disable access to such data.

The regulation in question applies *mutatis mutandis* to the securing of content published or provided by electronic means, with the caveat that the entity obliged to comply with a court's or prosecutor's request may also be the controller of the content.

Article 218a § 4 of the CCP provides that in the event that the publication or making available of the content referred to in § 3 constitutes a prohibited act referred to in § 1, the court or prosecutor may order the removal of such content, imposing an obligation to enforce the decision on the entities referred to in § 1 or § 3.

This measure aimed at securing evidence may not be appealed against. The Code of Criminal Procedure provides that an interlocutory appeal may be brought against a decision (order) which does not preclude the rendering of a judgement or is not a decision with respect to a precautionary measure (this refers to the preventive measures listed in

Chapter X of the Penal Code), only in cases prescribed by law (Article 459 § 2 of the CCP *in fine* in connection with § 1).

In conclusion, it is worth noting that Article 218a of the CCP owes its current shape to the Act of 20 April 2021 amending the Act – the Penal Code and certain other acts (Journal of Laws of 2021, item 1023), the purpose of which was, *inter alia*, to implement Directive 2017/541/EU on Combating Terrorism. Nevertheless, the legislators at the same time basically implemented, unknowingly or accidentally, some provisions of Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.

As it follows from the above discussion, Poland has only partially implemented the provisions of the directives imposing an obligation to develop measures to block and remove illegal content online. The provisions of Directive 2017/541 of 15 March 2017 on Combating Terrorism have been partially implemented, which, however, for the matter of tacking illegal content is not relevant due to the adoption by the EU of the TERREG Regulation, whose provisions are, after all, directly applicable.

Nothing has been done to implement Directives 2019/790 of 17 April 2019 Copyright and Related Rights in the Digital Single Market and 2011/93/EU of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography. Although, somewhat by coincidence, Article 218a of the Code of the CCP adopts analogous solutions to the latter.

References:

Machała, W. (2019) ACTA 2 czy Nihil novi? Pierwsze refleksje na temat dyrektywy Parlamentu Europejskiego i Rady o prawie autorskim na jednolitym rynku cyfrowym, *Monitor Prawniczy*, 18.

Markiewicz, R. (2021) Rozdział 9 odpowiedzialność dostawców usług udostępniania treści online (art. 17). 9.2.Treść dyrektywy. 9.2.5.Wyłączenie odpowiedzialności DUUTO. 9.2.5.1.Zasady generalne, In: Markiewicz, R. (ed.) *Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790* (Warsaw: Wydawnictwo, Wolters Kluwer Polska).

Matusiak-Frącczak, M. (2019) Rozdział 3. Polskie przepisy antyterrorystyczne a wymogi prawa Unii Europejskiej, In: Cała-Wacinkiewicz, E., Menkes, J., Nowakowska-Małusecka, J. & Staszewski, W. (eds.) *W jakiej Unii Europejskiej Polska – jaka Polska w Unii Europejskiej. Instytucjonalizacja współpracy międzynarodowej* (Warsaw: Wydawnictwo C.H. Beck), pp. 25-54.

Lewandowicz, M. (2017) Wybrane aspekty nowelizacji ustawy o grach hazardowych w świetle prawa unijnego, *Europejski Przegląd Sądowy,* 8, pp. 14-21.

Radoniewicz, F. (2021) Zwalczanie nielegalnych treści w Internecie - aspekty wybrane, In: Chałubińska-Jentkiewicz, K., Nowikowska, M. & Wąsowski, K. (eds.) *Media w erze cyfrowej. Wyzwania i zagrożenia* (Warsaw: Wydawnictwo, Wolters Kluwer Polska), pp. 155-188.

Threats Posed by Cyberterrorism to Public Administration

PAULINA KRAWCZYK

Abstract The stable functioning and development of a global information society depends on an open and, most importantly, secure cyberspace. In the modern world, which is becoming increasingly computerised, the number of attacks in cyberspace is constantly increasing. In order for an attack to be classified as a cyberterrorist attack, it must have the definitional elements of acts committed using violence against persons or property and cause considerable damage in order to generate fear and social unrest. In addition, such attacks must be carried out for a specific purpose, e.g., be politically motivated. Cyberterrorism is a form of warfare, which is primarily characterised by low operating costs. Cyberterrorism poses a significant threat to modern public administration. It interferes with the structure of internal state security. The most important objective of state functioning is to ensure the security of all its citizens. In order to eliminate cyberterrorism, it is extremely important to protect classified information.

Keywords: • cyberspace • cyberterrorism • public administration • CSIRT

CORRESPONDENCE ADDRESS: Paulina Krawczyk, Ph.D. student, War Studies University in Warsaw, Academic Centre for Cybersecurity Policy, Aleja Generała Antoniego Chruściela "Montera" 103, 00-910 Warszawa, Poland, e-mail: p.krawczyk@akademia.mil.pl.

https://doi.org/10.4335/2022.2.14 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

The protection of cyberspace has become one of the most addressed security issues. The stable functioning and development of a global information society depends on an open and, most importantly, secure cyberspace. Efforts to raise awareness in this area are undertaken in view of the rapid increase in the number of computer incidents and new types of threats. Poland, like European countries, has been presented with the challenge of ensuring the adequate protection of cyberspace. Apart from many positive aspects of the internet, the vast resources and its possibilities, cyberspace also carries enormous security threats. The more the world becomes dependent on modern technology, the greater the number of potential cyberterrorist attacks. The specific nature of the modern internet, which is extremely helpful to public administration users, may encourage terrorists to move their operations online. Technological progress in recent years has made cyberthreats a major concern for public administration. It might seem that cyberterrorist attacks have now displaced cybercrime, but nothing could be further from the truth. All critical infrastructures that rely on information technology are also at risk of cyberattacks.

In the modern world, which is becoming increasingly computerised, the number of attacks in cyberspace is constantly increasing, and what is more, they are very difficult to detect. The internet is a tool without which both citizens and the administration are unable to function. Thanks to computerisation, access to easily processed public information has certainly increased, as have communication possibilities.

There are numerous definitions of cyberterrorism in the literature. However, experts have highlighted the difficulties with defining this concept. The problem is that it is a diverse and dynamic phenomenon. Moreover, it occurs in many forms, and these forms change as human civilisation continues to evolve through technological progress (Olak, Krauz, 2014: 189).

The concept of cyberterrorism is widely believed to have been first coined by Barry Collin, an employee of the Institute for Security and Intelligence, who in the 1980s used this term by merging two concepts: cyberspace (Banasinski, 2018: 23) and terrorism (Szymczak, 1995: 463). According to him, cyberterrorism can be defined as the intentional abuse of an information system, network, or component toward an end that supports terrorist activities (White, Carlisle 1998: 10).

Dorothy Denning (Denning, 2002:79), on the other hand, argues that cyberterrorism is the unlawful attack on a computer network of users or a given information system aimed at instilling fear. Moreover, it can be said that cyberterrorist attacks are a form of an act of violence that cause serious damage to society and property (Fiktus et al, 2015: 481). Cyberterrorism aims to hamper, block or even distort the operation of IT systems. As a specific category of threats, it includes actions against communication and information systems undertaken to achieve specific terrorist objectives. Cyberterrorist attacks have already occurred in Poland many times. They mainly targeted government or computer systems in public administration, strongly destabilising the sense of security in the whole

country, not only within the area affected by the specific incident. This shows how strongly terrorist or, in this case, cyberterrorist activities affect people's sense of security (www.cybsecurity.org/wpcontent/uploads/2014/09/Do_rzeczy_nr38_2014_wybranowski.pdf) Cyberterrorism generally involves attacking computer systems using information technology. The use of such methods can cause computer systems to be blocked and lead to data loss (Aleksandrowicz, 2008: 23). The tools used for attacks include various forms of malware, such as viruses, bacteria, worms and server blocks, or conventional attacks. The above actions adversely affect cybersecurity, especially the security of state institutions, although terrorists may certainly cause damage in various areas of citizens' lives by attacking air traffic control systems, water supply systems, telecommunication systems, energy systems, water supply systems, transport and even power plants. These are just some of the areas that are a matter of concern for terrorists'. However, cyberterrorism is not just actions aimed at causing data loss. Cyberterrorism also manifests itself in propaganda and information campaigns, recruitment, the radicalisation of data exchange and sourcing. Terrorists use the internet to reach large numbers of people. Their main goal is to cause a disturbance of the peace in the form of protests and to disrupt the operation of government websites. In view of the constantly advancing computerisation, it is necessary to create effective systemic solutions at organisational and legal levels (Grzelak, Liedel, 2012: 136).

In order for an attack to be classified as a cyberterrorist attack, it must have the definitional elements of acts committed using violence against persons or property and cause considerable damage in order to generate fear and social unrest. In addition, such attacks must be carried out for a specific purpose, e.g., be politically motivated. Attacks on computers, networks or communication and information systems additionally entail serious damage to critical infrastructure, intimidation and attempts to force the government and public administration to yield to political and social demands. It should be remembered that cyberterrorism is a type of terrorism whose main distinguishing feature is that it is carried out in cyberspace and targets mainly communication and information systems or uses such systems.

Analysing all definitions, we can look at cyberterrorism in two ways. On the one hand – cyberterrorism as the use of information technology to mount a classic terrorist attack. On the other hand – cyberterrorism as an attack on computer systems as the main target of attacks rather than the tool to carry it out.

Cyberterrorism is a form of warfare, which is primarily characterised by low operating costs. To carry out an attack in cyberspace, no specialised equipment is required. Unlike terrorism, no weapons or explosives are used to mount a successful attack. Cyberterrorists only have a computer and internet connection.

Cyberterrorists also have a high degree of anonymity. It can be said that potential cyberterrorists can become anonymous online similarly to the standard internet users who go online on a daily basis. Cyberterrorists can easily adopt pseudonyms or impersonate

anonymous web users and make the identification of their real identity very difficult or even impossible. The difficulty here comes from the fact that terrorist organisations in the cyberworld have their own financial resources. Cyberterrorists are also well prepared for such attacks. Furthermore, they are characterised with great ease by which they mount cyberattacks. Cyberwarfare is now one of the modern battlefield dimensions. Technological progress has made it much easier for cyberterrorists to carry out their operations effortlessly. In addition, cyberterrorists know very well what they are doing and what their tasks are. Another characteristic of cyberterrorism is its global nature. A cyberterrorist attack can affect any country as long as it becomes the target of cyberterrorists. In the future, cyberterrorism may develop further still. One of the objectives of cyberterrorists is to draw the attention of media and to make sure the public is aware of their operations. Tracking and capturing cyberterrorists to punish them is extremely difficult but also expensive. To this end, special equipment is required and the people involved in combating this type of crime need adequate training and qualifications. A cyberterrorist can cause harm and hurt many people, not only from their own community, but also from many other countries around the world, without even walking away from their computer equipment. These people have the ability to cover their tracks so that their actions become as difficult to detect as possible. Last but not least, what makes cyberattacks increasingly popular is the fact that they involve a broadly defined information sphere. Cyberspace carries a considerable potential for furthering propaganda efforts. Modern technologies can be effectively used, for example, to disinform and manipulate public opinion.

Currently, three levels of cyberterrorist threats can be distinguished. The first is simple-unstructured, where cyberterrorists conduct basic hacking operations against individual ICT systems using tools created by someone else. The second level of threat is advanced-structured, where cyberterrorists conduct more sophisticated attacks against computer systems, as well as create by themselves, and modify, the hacking-tools they use to attack. They also have the capability to command and control attacks and refine attack methods. The third level is complex-coordinated, where cyber-terrorists conduct the most serious attacks, which are the most complex and coordinated, capable of causing mass-disruption against integrated, heterogeneous defence systems. They create and modify sophisticated hacking tools which they use to conduct future attacks. They also have command-and-control and learning capability (Oleksiewicz, 2018: 58-59).

The division of cyberterrorist threats by area of operation (Kowalewski, 2014: 28):

- attacks on military systems – these systems store information on the location of satellites, position of troops and military equipment, and on research on new types of weapons or communication systems. Most intrusions of this kind took place during the Cold War and the main perpetrators were usually agents of foreign intelligence services.
- attacks on enterprise systems – these systems store information relevant for a company's operations. It includes information about bookings, about a company's

clients and also about technologies used at work. The main perpetrators are usually employees who cooperate with competitors or feel the desire for revenge

- attacks on systems forming critical state infrastructure. The infrastructure includes the banking and financial, energy, telecommunication, water supply, transport and emergency services systems which store information relevant for national security. The perpetrators of such attacks may be the employees of companies related to these systems, and of course individual terrorists. At present, it is difficult to speak of elements of critical infrastructure which do not use technological support. The logical conclusion is that vulnerability to cyberterrorism is constantly increasing.

The use of the latest technology in the day-to-day functioning of the state means that the country may become more vulnerable to cyberterrorist attacks. Because of the Covid-19 pandemic that broke out in 2019, and other numerous problems occurring in the world, the community forgets more and more often about terrorist threats. They do, however, still exist and may gain in strength if using, for example, other threats such as the afore-said pandemic. This is confirmed, for instance, by Europol's latest report – "European Union Terrorism Situation and Trend Report 2021". This report emphasises that cyberterrorists use every opportunity to spread fear or propaganda. In this context, the Covid-19 pandemic and the accompanying increase in the use of the internet during this period proved to be a very favourable opportunity for them – on the one hand, to spread hatred, and on the other to integrate supporters. Since the use of the Telegram messenger is hampered, Islamists have struggled to find a universal communication channel and, as a result, their propaganda is scattered across various platforms. However, it still remains effective. The activity of other extremist groups, including extreme right and left-wing ones, is also increasing on the internet. Alongside traditionally addressed issues, they willingly take up new threads related, for example, to ecological, technological or pandemic issues (Analytical Report No. 33 of the Government Centre for Security).

At present, extremely rapid technological progress has taken place in the area of information technology. Nowadays it seems very difficult to function without instant messaging, search engines or access to email, especially on a daily basis. The dynamisation of the internet, as well as of the whole IT sphere, is the fastest-developing segment of social life (Hołyst, Jałoszyński, Letkiewicz, 2009: 120).

Some act for the benefit of times, many times facilitating and saving human lives, whilst others use the latest technology to kill and destroy, including state institutions (Pacek, Hoffman, 2013: 7).

In times of all these threats, the state must be extremely resilient to attacks and be aware of existing threats. The most important objective of state functioning is to ensure the security of all its citizens. For the state to function efficiently, all entities, institutions and services which are responsible for security in the country must be prepared for such threats. An inter-ministerial group of representatives from the Ministries of Digitalisation, National Defence, Internal Affairs and Administration, the Internal Security Agency, the

Government Centre for Security and the National Security Bureau have developed the Cybersecurity Strategy of the Republic of Poland for 2019-2024, which outlines "strategic objectives and relevant political and regulatory measures to achieve a high level of cybersecurity, principally a resilience to cyber threats of information systems used by operators of essential services, critical infrastructure operators, digital service providers and the public administration". This will also increase the level of national security (Cybersecurity Strategy of the Republic of Poland for 2019-2024 – Digitalisation of the Chancellery of the Prime Minister – Gov.pl Portal (www.gov.pl). The strategy is the result of the implementation of the Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, the so-called NIS Directive. Under the afore-said directive, in order to fight cyberterrorism effectively, activities should be coordinated primarily in the legal field, but also in terms of organisation. The protection of cyberspace is one of the fundamental tasks of public administration. An effective fight against cyberterrorism needs specialised institutions to use appropriate tools in order to monitor state security.

The authorities responsible for ensuring cyberspace security in Poland include the Ministry of the Interior and Administration, the Ministry of National Defence, the Internal Security Agency, the Military Counterintelligence Service and private entities.

In Poland, two institutions play a leading role in anti-terrorist activities: the Internal Security Agency (Journal of Laws of 2002) and the Police (Journal of Laws of 1990), which work closely together. The Internal Security Agency is a special service responsible for issues related to the protection of internal security of the state and its constitutional order. The main task of the Internal Security Agency is the protection of the state against planned and organised activities which might pose a threat to the independence and constitutional order of the Republic of Poland, as well as disrupt the functioning of the national government structure or jeopardise the basic interests of the country. The aim of this service is to combat various threats to the internal security of the state, such as the offences of espionage, terrorism, drug trafficking, organised crime or corruption. Measures to prevent the development of organised crime are based on granting powers to conduct operational and reconnaissance activities and criminal investigations to help to detect offences and prosecute perpetrators. Operational and reconnaissance activities, as well as analytical and information operations mainly serve the purpose of obtaining information to ensure state security and order as guaranteed by the Constitution of the Republic of Poland (Internal Security Agency – abw.gov.pl).

The Act on the National Cybersecurity System has established three Computer Security Incident Response Teams: CSIRT NASK, CSIRT GOV and CSIRT MON. Each of the teams is responsible for the coordination of incidents reported by entities assigned under the Act.

CSIRT NASK (nask.pl) – is led by the Research and Academic Computer Network – the National Research Institute.

The main tasks of the CSIRT NASK team include:

- recording and handling network security incidents;
- responding actively in a situation of immediate danger posed to users;
- cooperating with other CSIRT teams in Poland or worldwide;
- participating in national and international projects related to ICT security issues;
- conducting research on security incident detection methods;
- analysing malware and systems for the exchange of information about threats;
- developing proprietary tools for the detection, monitoring, analysis and correlation of threats;
- regular publication of the CSIRT NASK Report on the security of Polish internet resources;
- information and education measures aimed at increasing ICT security awareness.

The CSIRT NASK is obliged to coordinate incidents reported by the following entities:

- local government units;
- budgetary entities, local-government budgetary bodies;
- executive agencies, public-sector enterprises;
- public tertiary institutions and the Polish Academy of Sciences;
- the Office for Technical Inspection, the Polish Centre for Accreditation;
- the National Fund for Environmental Protection and Water Management, and regional funds for environmental protection and water management;
- commercial companies and partnerships carrying out tasks of general interest.

The CSIRT GOV (csirt.gov.pl) – led by the Head of the Internal Security Agency, it is the national-level CSIRT Team responsible for coordinating responses to computer incidents in the area indicated in Article 26 (7) of the Act of 5 July 2018 on the National Cybersecurity System.

The main tasks of the CSIRT GOV include the identification, prevention and detection of threats that compromise security and are important for the state's continuous functioning in terms of communication and information systems of public administration authorities or the system of ICT networks included in the uniform list of critical infrastructure facilities, installations and equipment, as well as communication and information systems of owners and possessors of critical infrastructure facilities, installations or equipment.

The CSIRT GOV is obliged to coordinate incidents reported by the following entities:

- public authorities, including government administration authorities, state inspection and law-enforcement authorities, and courts and tribunals;
- The Social Insurance Institution, the Agricultural Social Insurance Fund, the National Health Fund, the Polish Air Navigation Services Agency;
- the National Bank of Poland, Bank Gospodarstwa Krajowego.

The CSIRT GOV, together with the CSIRT NASK operate the ARAKIS-GOV system, which is an early warning system reporting threats emerging on the internet. This system has been developed through cooperation between the ICT Security Department of the Internal Security Agency and the CSIRT NASK team. The ARAKIS-GOV has been established to support the security measures protecting the ICT resources of public administration as a result of extending the ARAKIS system created by the CSIRT NASK by an additional functionality.

The CSIRT MON (csirt-mon.wp.mil.pl) – is led by the Ministry of National Defence. It is obliged to coordinate incidents reported by the following entities:

- entities subordinate to or supervised by the Ministry of National Defence, including entities whose communication and information systems or networks are included in the uniform list of critical infrastructure facilities, installations, equipment and services;
- entrepreneurs of special economic and defence significance, in respect of which the Ministry of National Defence is the authority that organises and supervises the performance of tasks aimed at ensuring national defence.

In addition to the afore-mentioned tasks of the teams, the Act on the National Cybersecurity System makes it possible to coordinate the activities of all CSIRTs in Poland. It enables them to cooperate with each other, jointly developing core elements of the procedures for handling computer incidents, the coordination of which requires cooperation. They specify, in cooperation with sectoral cybersecurity teams, how to cooperate with these teams, including how to coordinate the handling of incidents.

Simultaneously, CSIRT teams may, by way of agreement, entrust each other with the performance of tasks in relation to certain entities.

Another important element introduced by the Act in the area of cybersecurity is the possibility for CSIRT teams to perform device or software testing to identify the vulnerabilities which could be used to threaten the integrity, confidentiality, accountability, authenticity or availability of processed data, which may affect public safety or a vital interest of national security. On the basis of the afore-mentioned vulnerability testing, CSIRTs may provide recommendations to resolve vulnerabilities in devices or software used by entities within the national cybersecurity system (Computer Security Incident Response Team (CSIRT) – Digitalisation of the Chancellery of the Prime Minister – Portal Gov.pl (www.gov.pl).

The CSIRT GOV team is competent for handling incidents related to events of a terrorist nature, i.e., situations suspected to have developed as a result of an offence of a terrorist nature as referred to in Article 115 § 20 of the Act of 6 June 1997 – the Penal Code, or a threat of such offence (Article 2(7) of the Act of 10 June 2016 on Anti-terrorist Activities, Journal of Laws of 2019, item 796). Offences of a terrorist nature are defined as prohibited

acts committed in order to gravely intimidate many people, force a public authority of the Republic of Poland or of any other state or body of an international organisation to perform or refrain from performing certain activities, as well as to cause serious disturbances in the political system or economy of the Republic of Poland, another state or an international organisation – as well as a threat to commit such an act (the Act of 6 June 1997 – the Penal Code). The CSIRT MON is competent for handling incidents which are related to events of a terrorist nature and compromise the security of the national defence capabilities, affecting the Armed Forces of the Republic of Poland and organisational units of the Ministry of National Defence (Article 5 (1) (2a) of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, Journal of Laws of 2019, item 687). If it is determined that an incident the handling of which is coordinated by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV is related to the events referred to in paragraph one or two, incident handling coordination shall be taken over by the relevant CSIRT MON or CSIRT GOV (the Act on the National Cybersecurity System of 5 July 2018, Journal of Laws of 2018 item 1560).

In order to eliminate cyberterrorism, it is extremely important to protect classified information. Unauthorised access to this type of information may have serious consequences for the state. This is why cyberterrorists, when planning their attacks, initially use measures typical for cybercriminals. For example, they use techniques such as phishing, spoofing and hacking to extract data. This makes it easier to mount a complex and destructive cyberterrorist attack.

The key role in ensuring the protection of classified information is played by the Internal Security Agency and the Military Counterintelligence Service, which perform tasks related to the provision of personal security, i.e. conducting clearance proceedings, physical security, industrial security and ICT security.

Cyberspace has become a new security environment, prompting numerous changes, both in the pragmatic and in the legal and organisational dimensions of the functioning of security systems worldwide. In this context, it is particularly important to understand the dynamics of the changes in this environment. Building a legal system that constitutes the state's response to the opportunities and challenges of its presence in cyberspace is an extremely complex task.

There is a trend towards a shift from the traditional form of government-sponsored terrorism to a model in which the internet and other modern technologies are used, among other things, for propaganda, fundraising and recruitment of new members.

Cyberterrorism poses a significant threat to modern public administration. It interferes with the structure of internal state security. Nowadays, in times of globalisation, the expansion of societies, the flow of all goods, including information, this phenomenon should not be underestimated in any way. The state should take all available measures to prevent, at least to some extent, adverse phenomena such as cyberterrorist attacks. It is

the state's mission to implement appropriate systemic solutions in the area of prevention and to develop an early warning system against attacks. Institutions from both the public and private sectors should cooperate and coordinate actions to ensure security in cyberspace.

References:

Aleksandrowicz, T. (2008) *Terroryzm międzynarodowy* (Warszawa: Wydawnictwa Akademickie i Profesjonalne).

Banasiński, C. (2018) *Cyberbezpieczeństwo. Zarys wykładu* (Warszawa: Wolters Kluwer).

Denning, D.E. (2002) *Wojna informacyjna i bezpieczeństwo informacji* (Warszawa: Wydawnictwa Naukowo-Techniczne).

Grzelak, M. & Liedel, K. (2012) Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski-zarys problemu, *Bezpieczeństwo narodowe*, 22(2), p. 136.

Hołyst, B., Jałoszyński, K. & Letkiewicz, A. (2009) *Wojna z terroryzmem w XXI wieku* (Szczytno: Wydawnictwo Wyższej Szkoły Policji).

Kowalewski, J. & Kowalewski, M. (2014) Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa, *Telekomunikacja i Techniki informacyjne*, (1-2), p. 28.

Olak, A. & Krauz, A. (2014) Zjawisko terroryzmu we współczesnym świecie, *Kultura bezpieczeństwa. Nauka-Praktyka-Refleksje*, 15(15), p. 189.

Oleksiewicz, I. (2018) Cyberterroryzm jako realne zagrożenie dla Polski, *Rocznik Bezpieczeństwa Międzynarodowego,* 12(1), pp. 58-59.

Pacek, B. & Hoffman, R. (2013) *Działania sił zbrojnych w cyberprzestrzeni* (Warszawa: Wydawnictwo Akademii Obrony Narodowej).

Fiktus, P., Malewski, H. & Marszał, M. (2015) *Rodzinna Europa. Europejska myśl polityczno – prawna u progu XXI wieku* (Wrocław: E-Wydawnictwo, Prawnicza i Ekonomiczna Biblioteka Cyfrowa, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego).

Szymczak, M. (1995) *Słownik języka polskiego, t. III* (Warszawa: Wydawnictwo Naukowe PWN).

White, K.C. (1998) *Cyber-Terrorism: Modem Mayhem* (Carlisle: U.S. Army, War College), available at: apps.dtic.mil/sti/pdfs/ADA345705.pdf (January 5, 2022).

Cybersecurity and Cybercrime in Hungary During the COVID-19 Pandemic

KITTI MEZEI & CSABA KRASZNAY

Abstract In March 2020, the whole world was hit by home office in one fell swoop, without the right IT tools and knowledge to work remotely. Deploying remote access and cloud-based services was nowhere near as easy, neither from a technical nor human point of view.The first warning sign that the digital switchover due to COVID-19 could have cybersecurity implications is perhaps best followed through the Spring 2020 calvary of the Zoom application. In 2021, Hungarian users could also find out about the security of endpoints from direct events that caused a lot of press coverage. The safe operation of education systems is a major administrative and technical challenge for the operators of individual institutions. In addition to mass phishing attacks, targeted spear-phishing attacks have also occurred, particularly taking advantage of the uncertainty caused by the coronavirus epidemic and the large number of people working from home. The first and most crucial issue is the emergence of certain applications of artificial intelligence in cybercrime. The second important question is how the perpetrators have suddenly improved their operational planning and operational security for committing cybercrime. The third concern relates to cooperation between states.

Keywords: • COVID-19 • cybersecurity • cybercrime • deepfake • fake news • online fraud • phishing malware • distance learning

CORRESPONDENCE ADDRESS: Kitti Mezei, Ph.D., Research Fellow, Centre for Social Sciences, Institute for Legal Studies, 1097 Budapest, Tóth Kálmán u. 2-4, Hungary; Assistant Professor, Budapest University of Technology and Economics, Faculty of Economic and Social Sciences, Department of Business Law, 1117 Budapest, Magyar Tudósok körútja 2, Hungary; Postdoctoral Researcher, University of Public Services, Institute of Cybersecurity, 1083 Budapest, Ludovika tér 1, Hungary, e-mail: mezei.kitti@tk.hu. Csaba Krasznay, Ph.D., Director, Associate Professor, University of Public Services, Institute of Cybersecurity, 1083 Budapest, Ludovika tér 1, Hungary, e-mail: krasznay.csaba@uni-nke.hu.

https://doi.org/10.4335/2022.2.15 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 COVID-19 pandemic and cybersecurity

According to a meme often shared by IT professionals recently, the main source of digital transformation for companies was neither the CEO nor the IT manager but COVID-19 (High 2021). It would be difficult to argue with the reality of this, as the relevant data proves it. For example, according to WeAreSocial's summary, between January 2020 and January 2021, the number of Internet users increased by 7.3%, equals 316 million people, the number of social media users by 13.2%, equals 490 million people. Meanwhile, the world's total population grew by only 1%, equal to 81 million people (Kemp, 2021). The relevant figures esteeming Hungary's digital transformation in the European Union's Digital Economy and Society Index (DESI) 2021 show similar results, such as the stagnant 64% to 70% of eGovernment users and the number of corporate users of cloud services rose from 11% to 17%, which is still well below the European average (European Commission, 2021a).

So, there is no question that our subjective feeling that IT surrounds us is completely correct. Whether it is our work, learning, or communication, digital tools and services are unavoidable. And what is unavoidable, if it is not used properly or used inappropriately or with malicious intentions, it can lead to serious social problems.

This is faithfully reflected in the trends related to cybercrime, which clearly show that organised crime groups have adapted to the digital transition of potential victims and have developed crime patterns that can maximise their benefits in acts against individuals and organisations that have just latched on online services. These trends are perfectly highlighted in Europol's annual Internet Organized Crime Threat Assessment (IOCTA) 2021 report, which makes it easy to point to global and domestic challenges.

2 The home office posed cybersecurity challenges

In March 2020, the whole world was hit by home office in one fell swoop, without the right IT tools and knowledge to work remotely. No wonder there has been a drastic increase in the demand for web conferencing applications through which meetings could be conducted and after which everyone learned the name Zoom or Microsoft Teams. After that, creating secure access to enterprise resources soon became a serious need, leading to increased use of cloud services and the use of virtual private networks (VPNs) on a daily basis. In this connection, the information security specialists of the companies have gained short-term experience that the user endpoints (smartphones, tablets, laptops) very often do not even meet the basic security requirements. Then, as a final blow, it also had to be realised that there is no telecommuting without IT infrastructure that is resilient to cyber threats (Europol, 2021).

The first warning sign that the digital switchover due to COVID-19 could have cybersecurity implications is perhaps best followed through the Spring 2020 calvary of

the Zoom application. The first security problems of the solution, which suddenly became very popular, were highlighted by researchers in mid-March, followed by more and more news almost daily. Without wishing to be exhaustive, the following announcements followed one another:

- **March 30**
  The world is getting to know the phenomenon of zoombombing when unauthorised people enter video conferencing due to a software authentication error.
  It also turns out that Zoom is sending user data to Facebook.
- **April 1**
  Researchers point out that Zoom uses inappropriate end-to-end encryption.
- **April 2**
  It turns out that by exploiting a software error, passwords stored in Windows used to make calls could be stolen.
  Unauthorised access to other users' cloud-stored Zoom data is achieved.
- **April 3**
  Zoom-related phishing pages appear in bulk.
  Analyses show that the company is using an inappropriate encryption algorithm.
  Due to increased user demands, the company is starting to use new cloud servers located in China, which means several calls important to national security are going through this country.
- **April 6**
  Illegally recorded Zoom conversations are appearing on YouTube.
- **April 7**
  Zoom gets banned by several government agencies.

After that, Zoom spent a total of 3 months improving the security of its service, setting an example for its competitors. Since then, there have been no major security concerns about online conferencing services. We can even attribute a number of exemplary privacy measures to them, such as blurring the room image in the camera and replacing it with a virtual background.

Deploying remote access and cloud-based services was nowhere near as easy, neither from a technical nor human point of view. According to the perspective of information security, this meant that the company had to be „opened up" to the world, to the Internet. There was a serious fear that the range of people accessing corporate information and the path of the information that escaped would become uncontrollable. While technical best practices are, of course, given to implement secure remote access, unfortunately, cybercriminals have begun to exploit the flaws of these solutions. For example, as mentioned in the IOCTA 2021 report, gangs that spread ransomware actively exploit vulnerabilities in VPN solutions and Microsoft Remote Desktop Protocol (RDP) to distribute malicious code. It should also be mentioned that according to HaveIBeenPwnd.com's records, there are more than 11.6 billion leaked, traceable user

accounts and passwords on the Internet, while hundreds of millions more access are being traded on the darknet.

In 2021, Hungarian users could also find out about the security of endpoints from direct events that caused a lot of press coverage. One such attack, which affected almost everyone, could be linked to malicious code called FluBot. During the infection, the victim first received an SMS that his or her package was arriving, but he or she would need to download an app to track it. After installation, the application had access to the data stored on the victim's phone, including the phone numbers. It collected the contacts and automatically transmitted the phishing SMS to them. For the infection, the victim had to actively click on the attached links and permission requests, so in general, the biggest threat lurking at the endpoints is the user itself, which raises the question of how much risk companies take regarding their complete security when allowing remote access to individually owned devices (National Cyber Security Center, 2021). Another such event is the revelation of Pegasus spyware developed by the NSO Group. Although this has only been used in a targeted manner against properly selected individuals, the case points out that an endpoint device and the data stored on it can be accessed remotely without the victim having to click on anything (Marczak, 2021).

The availability of infrastructures and, incidentally, organisational data assets are being tested by extortion-type attacks, in particular, ransomware and Distributed Denial of Service (DDoS) attacks with extortionist aim. Although these types of attacks are not new, their numbers have increased significantly during COVID-19. The modus operandi has changed, making it virtually impossible for most organisations to defend against them. An example of both cases occurred in Hungary. In April 2021, the most prominent car parts retailer, Unix Auto, fell victim to ransomware, and in November 2021, MediaMarkt's online sales became impossible due to similar reasons. In the first case, the infrastructure was Hungarian; in the second case, the international centre became the target, which also affected the Hungarian operation. Most Hungarian media service providers got to know about the DDoS attacks in the autumn of 2021, when their websites became inaccessible for hours.

3 Distance learning and cybersecurity

In March 2020, Hungarian public education was switched to absence digital education in one day. Tertiary education had two weeks. According to the data of the Hungarian Central Statistical Office in 2019, this meant 1.8 million users in Hungary, most of whom have never experienced learning via the Internet before (Hungarian Central Statistical Office, 2019). Of course, no actor in education was prepared for this rapid shift, as although many good practices were widespread and excellent foreign examples were available, their profound adaptation was not encouraged by legislation or the National Core Curriculum. Legally, nor the IT infrastructure was ready to accommodate this nearly two million people, and the state-developed e-Kréta system got able to serve the digital

needs of public education only roughly a year after the outbreak of the pandemic (Hoffman, 2021: 150), meanwhile taking classes via the Internet continued using foreigner services (Microsoft Teams, Google Meet, Zoom).

The review of 1488/2016. (IX. 2.) Government Decree on the Establishment of a Secure Internet Service for Children, on Conscious and Value-Creating Internet Use and on Hungary's Digital Child Protection Strategy shows the unpreparedness of the Hungarian education system to distance learning, which is safe and considers data protection. The detailed strategy issued on the basis of the government decree shows exactly what affairs the legislator planned to solve by 2020. It contains a number of important issues, which, although, could have contributed to overcoming some of the sub-problems, however, the document does not specifically address the concepts of distance and absence learning or the digital agenda. There is no trace of increasing the security of computer use at home or even improving the privacy and information security skills of educators in the toolkit. There is only one measure in the text, the implementation of which might have been useful at the time of the declaration of the state of danger: „Preparation and dissemination of information on child protection rules according to the Act CVIII of 2001 on Electronic Commerce and on Information Society Services and consumer protection law enforcement in relation to online commerce, furthermore up-to-date information on online child protection legislation, defensive options and media literacy programs on the website of each public education institution theorem" (Hungary's Digital Child Protection Strategy, 2016).

It is a feature of the digital work schedule that students, teachers, educators typically communicate with each other through their own device on a platform managed by an external service provider, sharing data and information that are considered personal. It can be seen that there are serious concerns about a situation where a minor child joins an online classroom via video, while his or her living space is visible in the background, all on a platform that the teacher has registered for free, thus approving the terms and conditions that the service provider is clearly designed to make the most of the data passing through the platform. From a privacy perspective, it is also a questionable practice for a teacher to request a video from a child to prove that he or she has completed a physical education class, who shares this with their teacher through a cloud provider. By storing the video, data processing takes place in an environment where data protection regulations are not clear. Since most educators decided to pass the curriculum at their own discretion during the first period of absence education, there were some particularly bad practices, such as requiring a child under the age of 13 to register on Facebook with a teacher's expectation. Not only did the parents' previous educational goals have to be violated, but also the social network's own rules of use.

The safe operation of education systems is a major administrative and technical challenge for the operators of individual institutions. Many elementary and high schools do not have a document regulating IT security, as a result of which the processes for operating an IT

system are not defined. Instructors who operate school IT systems often only on a part-time or class reductive basis are required to ensure that the infrastructure is operational and to assist the school administration involved. The optimal solution in this situation is to outsource the operation of IT specialist systems, thus using a centralised service where the operational tasks are performed by qualified professionals. In case of systems where external service is not available, they try to provide a solution by building their own system, the long-term safe operation of which can be risky for them.

In tertiary education, in most cases, there is a company-level IT background available to support teaching and research work, which is operated either by a central organisational unit or by independent IT staff in each organisational unit. The vast majority of tertiary educational institutions have IT security regulations, and although they are not subject to uniform content regulations, most of them show the spirit of Act L of 2013 on electronic information security. When purchasing systems, the supplier also provides some training so that operators know and are able to operate them to some extent. Many institutions have contracts that provide professional support beyond the general operational tasks.

In light of all this, it is not surprising that the number of cybercrimes has risen significantly as children have been at home and used more digital devices than before, and educational institutions have been forced to maintain educational infrastructure without adequate resources (Coman and Mihai, 2021: 4). The IOCTA 2021 report, for instance, identifies the education sector as one of the main targets of ransomware attacks. Unfortunately, however, the drastic increase in sexual abuse of children highlights the particular problems of using the Internet for students' entire lives. Europol warns that online grooming has grown sharply on children's favourite social networks and gaming platforms, while the spread of children's own images is also a matter of serious concern. Both adults and children are at risk of online sexual extortion (sextortion), but the latter is particularly. In this case, the perpetrator wheedles him- or herself into the trust of the child (e.g., pretends to be a juvenile and befriends the child, shows him or her sexually explicit material to reduce his or her sexuality-related inhibitions), and exploits his or her vulnerability (Powell and Nicola, 2017: 122-124). The perpetrator does this in order to access sexually explicit images or videos of the child, which is eventually followed by a blackmail phase, when he or she is forcing, extorts his victim to do a sexual favour for him or her or to send additional compromising images or videos of him- or herself. If the victim does not comply with the request, the extortionist threatens to share the recording he or she already has (for example, through social media) and puts the victim under his or her control (Europol, 2014: 30). Without complete social isolation due to COVID-19, these two trends would presumably be less significant.

4 The COVID-19 pandemic and cybercrime

The COVID-19 virus crisis has been exploited in the online sphere and has become a major "bait" for offenders. The emergence of a crisis always brings new circumstances that provide an ideal environment for cybercriminals. For example, when Italian citizens could apply for coronavirus benefits, some hackers attacked Italy's social security website, causing a one-day shutdown.

During a pandemic, there is an alarming increase in the number of cyber-attacks against healthcare organisations. These threats have affected hospitals (for example, in the Czech Republic, a healthcare facility carrying out testing was paralysed by a ransomware virus), the World Health Organisation (WHO), whose servers have been hacked, and even companies at the forefront of vaccine development, as well as the European Medicines Agency (Palicz, Bencsik and Szócska, 2021: 84-85.). The healthcare sector lags far behind in cybersecurity, with a lack of digital skills among staff, outdated software and inadequate regulation and enforcement (Chigada, Madzinga, 2021).

In addition, perpetrators often target mobile devices, for example, to develop – or manipulate –apps that appear to track the spread of the coronavirus. In reality, the application infects the device with malware and collects personal data, credit card information, etc. (Collier et al., 2020: 5).

5 Phishing and malware

In parallel with the emergence of the coronavirus epidemic, phishing has also been on the rise. COVID Internet domain registrations have recently increased significantly, in many cases created for phishing. The fake websites appear to be real sites of real organisations but are used to distribute malware. Several COVID-19 phishing campaigns have been identified, attempting to exploit people's fear of the virus and trick them into opening malicious attachments, even on behalf of local or international health organisations (the WHO or the National Surgeon General). For example, COVID-19 phishing packages (e.g. infected programs disguised as a map showing the spread of the virus) are already available on the darknet. The subjects of these phishing emails include analyses of specific industries and official advice from health authorities on the coronavirus epidemic, as well as counterfeit products. The email attachments include ransomware, remote access Trojans and keystroke recorders installed on unwary users' computers and mobile phones (Guirakhoo, 2020).

As the number of infected people has increased, scams have emerged in which people are contacted on behalf of local hospitals claiming to have been infected. In other cases, attempts are being made to deceive people by using the digital COVID certificate issued by the European Union. The perpetrators also use malicious content hidden in the attachment in these cases.

The weakest link in cybersecurity is the human being. In most cases, the victim is behind every successful attack, so perpetrators often prefer social engineering attacks such as phishing to technical solutions.

According to Google, in March 2020, fraudsters sent 18 million phishing emails per day to Gmail users on COVID-19. In April, the tech company blocked more than 100 million phishing emails per day, nearly a fifth of which were related to the COVID-19 virus scam (Tidy, 2020). Emerging technologies such as artificial intelligence can make cyber-attacks more effective. Perpetrators can use it to develop malware, increase the effectiveness of ransomware or more targeted social engineering attacks, and circumvent image recognition and voice recognition, among other things. Europol is already calling for so-called "AI-as-a-service", or AI as a service, which could already be used for malicious purposes. (Cerulus, 2021 and see more Caldwell et al., 2020: 1–14).

Malicious programs and hacker attacks may constitute a criminal offence according to the Hungarian Act C of 2012 on the Criminal Code (hereinafter referred as to Criminal Code). The Hungarian Criminal Code in Section 423 contains the offence of breach of information system or data, which covers conducts criminalised under international and EU legislation (Budapest Convention on Cybercrime and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems). According to Subsection (1), any person who gains unauthorised entry to an information system by compromising or defrauding the integrity of the technical means designed to protect the information system or overrides or infringes his or her user privileges is guilty of a misdemeanour punishable by imprisonment not exceeding two years. If it is committed intentionally by unauthorised access, for example, by a person who does not have access to the system (so-called hacking) or by exceeding or violating the limits of his/her access rights by remaining inside (for example, by using the password of another colleague who has access to the system in his/her capacity as an employee). Notably, the offence must be committed by breaching or circumventing a technical measure that provides protection (this means that the information system must have active protection, such as a password or other means of protection, for the offence to be established). The offence does not constitute a purpose, and therefore it is not a condition of the crime that it is committed for gain, damage or similar purposes. Nor is it a requirement that the offender subsequently performs any operation on the data stored in the information system or even interfere with the system's functioning. Therefore, unauthorised access is a criminal offence in itself (mere hacking). If this is followed by further unauthorised operations, such as deleting data or making it inaccessible, one of the following paragraphs is already triggered and merges into the more serious paragraphs of breach of information system or data. It is possible to cause damage to information systems in various ways. For example, someone who gains unauthorised access to the system could send a command to delete files necessary for the operation or a system shutdown. These cases are governed by Section 423 Subsection (2) point a) of the

Criminal Code, which provides that anyone who disrupts the use of the information system unlawfully or by way of breaching his or her user privileges is guilty of a felony punishable by imprisonment not exceeding three years.

Unauthorised interference with the operation of an information system or interference in breach of the limits of its lawfulness is also punishable under this offence. For example, it is not necessary for the offender to have access to the information system in question, as it is sufficient to interfere with its proper functioning in any way, regardless of the duration and extent of the interference, such as launching a DDoS attack, which results in the website of a bank or other service provider being rendered inaccessible.

According to Subsection (2) point b), anyone who alters or deletes, or renders inaccessible without permission, or by way of breaching his user privileges, data in the information system is guilty of a felony punishable by imprisonment not exceeding three years.

In addition, various manipulations of data in the information system are also prohibited: if data in the information system is altered, deleted or made inaccessible without authorisation or in violation of its authorisation (for example, as in the cases mentioned above, by infecting the system with malware, such as the trend in recent years to use ransomware, (Wall, 2021) or by further manipulation of data following unauthorised access).

An aggravated offence may be established and punishable for imprisonment between one to five years for a felony if the acts defined in Subsection (2) involve a substantial number of information systems, but the law does not define what constitutes a significant number, so it is for judges to develop a practice in this regard. An excellent example of an aggravated case is DDoS attacks. The attacker attempts to connect to the attacked computer by using hundreds or thousands of users' information systems controlled remotely by the attacker. Many data requests and transmissions are sent at once paralyses the attacked information system, which may exhaust the notion of a significant number of information systems.

In the other aggravated case, the penalty shall be imprisonment between two to eight years if the criminal offence is committed against works of public concern. Among the interpretative provisions, the Criminal Code defines in Section 459, point 21, by way of example, what constitutes as works of public concern: utilities, public transport establishments, electronic communications networks, logistics, financial and IT hubs and operations necessary for the performance of the tasks of universal postal service providers carried out in the public interest (e.g. financial institutions) and plants producing war materials, military items, energy or basic materials destined for industrial use. The problem with this is that the notions of critical infrastructure and works of public concern as used in the EU law (Directive 2013/40/EU on attacks against information systems) do not overlap, so the qualification of the offence can be controversial, especially in the case

of cyber-attacks on institutions of social welfare, public health. This is also important to draw attention to because, since 2017, Hungary has also introduced an electronic health system. All personal data and institutional care documents are stored electronically, thus increasing the risk of possible cyber-attacks.

In the case of spyware, the offence of illicit access to data [Section 422 (1) (e) and (d) of the Criminal Code] may arise if the data or the content of communications handled in the information system are secretly intercepted to obtain unauthorised knowledge of personal data, private secrets, trade secrets or business secrets, and the intercepted data are recorded by technical means.

In the context of the collection of bank card data and personal data, fraud (Section 375 of the Criminal Code) and misuse of personal data (Section 219 of the Criminal Code) are typically committed using the information system. According to Section 219 Subsection (1), a person who, by violating a provision laid down in an Act or a binding legal act of the European Union on the protection or processing of personal data and for gain or causing significant harm to interests, a) processes personal data in an unauthorised manner or in deviation from the purpose of processing is guilty of a misdemeanour and shall be punished by imprisonment for up to one year.

In cases when unknown persons create a fake profile on the social media site using the user's name and photos are considered criminal cases. Through this pseudo-profile, the perpetrator identifies the real friends of the impersonated user and sends messages and posts messages on behalf of the user. The aim is often to discredit the person concerned, tarnishing their reputation in the eyes of others, and this can result in significant damage to their interests. It is also possible that the personal data of others is used to commit crimes, for example, to defraud unsuspecting users of money or credit card details through a fake profile on social and online dating sites (romantic fraud) or e-commerce platforms.

6 Online fraud

In addition to mass phishing attacks, targeted spear-phishing attacks have also occurred, particularly taking advantage of the uncertainty caused by the coronavirus epidemic and the large number of people working from home. These emails are created in both content and form so that their unique features do not arouse suspicion. The attack is always preceded by a study of the intended targets (e.g. a preliminary assessment of their workplace, behaviour, and organisational structure). The perpetrators often pose as company executives or employees, business partners – business email compromise or CEO fraud – and send an email to the person responsible for the finances (e.g. a financial controller or accountant) asking them to carry out an urgent bank transaction. This step may be followed by further emails or even phone calls to confirm the need for the transaction by presenting themselves, for example, as a trusted business partner or lawyer. It is also common to hack into a company's mail system and gain access to valuable

information (e.g. who the targeted company has a supplier or other contractual relationships with, address lists, business correspondence, etc.) that may facilitate a targeted attack. As highlighted by the FBI's report, these attacks are highly costly, which estimates they caused 360 million dollars in 2016 and $675 million dollars in 2017 (U.S. Department of Justice, 2018, p. 36). These cases typically fall within the traditional offence of fraud. According to Section 373 of the Criminal Code, it is committed for illicit gain by defrauding a natural person and causing financial damage.

Taking advantage of the shortage of goods and the general fear, several online trading platforms have been set up to sell sought-after products such as sanitary masks, hand sanitisers and tests. However, customers never receive the products after paying the bill, and the fake online store operators disappear with the money. Such cases have also occurred in Hungary, where criminals have accessed the e-mail account of a person unknown to them without authorisation and then used the e-mail account by changing the password. They used the email account to register on an Internet portal and advertised respiratory protection masks, taking advantage of the epidemic situation. The perpetrators gave bank account numbers to the persons who had signed up for the advertisement, to which the victims transferred the money but did not send the ordered mouth masks because they did not have them. They applied for advertisements from different parts of the country (Prosecutor's Office of Hungary, 2021 and see more about online fraud cases: Wan Fei Ma, McKinnon, 2021; Murrar, 2021, and Buil-Gil, Zeng, 2021).

The person is liable for breach of information system or data (Section 423 of Criminal Code) because he did not have the right to use the e-mail account. He logged in and even changed the password by circumventing the technical measure. They are also liable for traditional fraud because they misled natural persons and caused them harm. In this case, the person does not cause damage through an operation using an information system and therefore cannot be held liable for fraud utilising an information system. For example, suppose you access your online banking account and make an unauthorised transfer or purchase using the obtained credit card details. In that case, you are committing fraud using the information system, as the central element of the offence is the information system and not the misrepresentation or fraud of the natural person.

In addition, a new series of frauds has emerged in Hungary that exploited the growing popularity of home delivery in the wake of the epidemic and restrictive measures. SMS messages were sent on behalf of courier services in response to the increase in online shopping. Unlike emails, SMS only shows a phone number, with no sender address to check (smishing). In all cases, the SMS requesting us to track your parcel contains a link that appears to take you to a known courier service when opened. Here, the unsuspecting user is asked to download and install an application to track their parcel, which is malware (such as the FluBot above) and collects data on the mobile phone, mainly bank IDs, cryptocurrency or credit card details.

In the UK, there have been cases of smishing that followed government announcements such as COVID-19 promising financial assistance and directing the public to a fake government website requesting bank card details. In another case, parents were targeted and promised help with free school meals but were also asked for bank details in return (Lalliea et al., 2021).

In parallel with the emergence of new security measures (e.g. strong identification systems, two-factor authentication, which banks are obliged to use), criminals are also trying to circumvent this through so-called SIM-swapping. Through social engineering or phishing, they obtain personal data and then block the old SIM card on behalf of the victim at the mobile phone service provider and request a new one to access various bank or other user accounts (Europol, 2020: 44–46).

Similar cases have been reported in Hungary. Victims were attracted by an advertisement for a house for sale at an excellent price in one such case. The advertiser informed them by telephone that the discounted price was because he needed money urgently because of family circumstances. He also indicated that the relative would soon show the apartment to other interested parties. Only one photo had been uploaded to the ad site but promised to send more pictures and a video by e-mail. The victims requested to receive the images through a service for sending large files, but the advertiser offered other free software for this purpose. The victims had no idea that the software could be misused on their computers. The software allowed the advertiser to establish a remote desktop connection between the computers. He then waited for the victims to log into their Internet bank account. This alone is not enough, because the only way to access the bank account is through two-factor identification, i.e. to enter and access the bank account after entering the code received in the SMS, in addition to the bank ID, and to do this, the perpetrator had to have control of their phone. The mobile phone provider said that an unknown person had initiated the exchange of SIM cards belonging to the victim couple's company subscription at one of their shops. The unknown person in charge claimed that they had been stolen and asked for the original cards to be blocked. The victims' phones then went silent. In addition, the unknown person presented a forged signature of the victims' company. The money in the victims' bank accounts was then accessed via the Internet banking service, and the nearly 85 000 euro was converted into bitcoin after repeated transfers (Horváth, 2020).

If the perpetrators obtain only the Internet banking login data and use them to cause damage using a transaction in the information system (e.g. by making a bank transfer), then the offence of fraudulent misuse of data by using the information system is committed under Section 375 Subsection (1), the offence of information system fraud. According to this Subsection, any person who, for unlawful financial gain, introduces data into an information system, or alters or deletes data processed therein, or renders data inaccessible, or otherwise interferes with the functioning of the information system, and thereby causes damage, is guilty of a felony punishable by imprisonment not exceeding

three years. The offence is an important complement to the traditional offence of fraud (Section 373 of the Criminal Code) because it covers fraudulent conduct that causes damage to property by direct use of the information system, and therefore does not involve the deception of a natural person, which is essential to establish fraud.

If they obtain credit card data without authorisation and use the information system to cause damage (e.g. purchasing in an online shop using the credit card). In that case, they may be liable for the fraudulent use of an electronic cash substitute payment instrument as defined in Subsection (5). This offence has no offence form - as is typical for other offences against property - and the basic cases cover damage ranging from one forint to five million forints. According to this Subsection, any person who causes damage by using a counterfeit or forged, or unlawfully obtained electronic payment instrument, or by accepting payment with such payment instrument shall be punishable.

Nemzeti Média- és Hírközlési Hatóság (National Media and Infocommunications Authority) (hereinafter referred as to NMHH) has been monitoring the practices of service providers with SIM card swapping in such cases. There have been cases of abuse that have caused considerable financial damage based on access to victims' bank confirmation SMSs. To keep our data and assets safe, a simple authorisation is no longer enough when it comes to changing our SIM cards. The NMHH has asked Telekom, Telenor and Vodafone to introduce new procedures after monitoring their practices. The telecoms authority and the operators expect tightened measures to reduce this type of abuse significantly. We can expect to see checks on the SIM card is replaced, delayed activation of the new card, requiring authentication in case of authorisation, but also sending verification codes and information SMS (NMHH, 2021 and see more about SMS-swapping: ENISA, 2021).

7 Deepfake and fake news

Finally, the rise of deepfake technology is worth mentioning, which is relatively new and poses an increasingly serious challenge to society. In the case of deepfake, an algorithm can replace the facial image in a video recording of a person with the facial image of another person, which can be deceptive to anyone. In addition to the harm caused to the individual (see revenge porn or content generated by artificial intelligence used for fraud), deepfake can contribute to disinformation (Whyte, 2020), distort democratic decision-making, and manipulate the electoral process, eroding public trust exacerbating divisions in society (Kirchengast, 2020). Protection against the coronavirus can also be hampered by fake news (e.g. content shared on social media, posts about the virus and vaccines). Therefore, new criminal conduct (Article 337 of the Criminal Code) has been added to the offence of fearmongering. According to Subsection (2), a person who, during the period of a special legal order and in front of a large audience, states or disseminates any untrue fact or any misrepresented true fact that is capable of hindering or preventing the efficiency of protection is guilty of a felony and shall be punished by imprisonment for

one to five years. The Hungarian Government introduced a state of emergency due to the coronavirus pandemic. There are increasing cases when people publish a piece of writings on the Internet that could impede the effectiveness of the protection against the coronavirus. These give rise to suspicion of the abovementioned criminal offence. Disinformation is still a major issue in the COVID-19 public debate. As a result, many have chosen not to believe in the scientific data, acknowledge COVID-related health risks and/or be vaccinated against the disease (European Commission, 2021b).

8 Summary

One of the key characteristics of cybercrime is its rapid adaptation. With the attacker infrastructure, know-how and billions of potential victims constantly available, it is a matter of finding the right theme to base an attack. The rapid digitalisation resulting from COVID-19 has created an unprecedented opportunity for criminal groups to use existing techniques to target a common theme. We saw familiar patterns in a coronavirus costume in the first pandemic period. But the phase from autumn 2020 onwards has brought frightening new developments, the rapid effects of which have already been felt through the evolution of ransomware or attacks on supply chains. But its long-term consequences are still to be seen.

The first and most crucial issue is the emergence of certain applications of artificial intelligence in cybercrime. The involvement of deepfake in online fraud is already a sign that AI is a technology available to anyone, but when will the most prominent groups start to exploit it to 'train' algorithms from stolen data? Remember, a criminal organisation is not hampered by data protection rules such as GDPR. They can get more accurate profiles and organisational information with the right knowledge than the best data analytics firms. And based on what they know about defensive solutions, they may develop attack algorithms that even the most sophisticated organisation is defenceless against.

The second important question is how the perpetrators have suddenly improved their operational planning and operational security for committing cybercrime. Although the link between intelligence agencies and criminal groups has existed since states have been conducting covert operations, and cyberspace operations are no exception, history teaches us that the most dangerous mix is when trained intelligence operatives turn to crime. This is evidenced by the Mexican drug war, where one of the most dangerous groups, Los Zetas, was founded by former secret service agents or the Islamic State terrorist organisation, in which former Iraqi intelligence agents were actively involved. Given that the high-profile cybercrimes of 2021 were committed in ways previously only used in state cyber operations, it is feared that intelligence knowledge has been transferred to these groups.

The third concern relates to cooperation between states. The ability to fight cybercrime is diminishing from North to South, the willingness from West to East, as a practising

investigator once put it. Unfortunately, this is borne out by the facts, as Russia and China did not participate in the October 2021 meeting held by President Biden to prevent the spread of ransomware. However, the answer to a question about Russia's absence suggested that the two governments had begun cooperating (The White House, 2021). Given the abundance of perceived state operations at the beginning of the COVID-19 period, it is questionable how genuine this willingness to cooperate is and how it can be sustained in emergency situations. Without cooperation, cyberspace peace cannot be achieved, and joint responses to the issues raised earlier cannot be provided.

Acknowledgment:

The research was supported by the Ministry of Innovation and Technology NRDI Office within the framework of the FK_21 Young Researcher Excellence Program (138965) and the Artificial Intelligence National Laboratory Program.

References:

Buil-Gil, D. & Zeng, Y. (2021) Meeting you was a fake: investigating the increase in romance fraud during COVID-19, *Journal of Financial Crime*, 29(2), pp. 460-475, https://doi.org/10.1108/JFC-02-2021-0042.

Caldwell, M., Andrews, J.T.A., Tanay, T. & Griffin, L.D. (2021) AI-enabled future crime, *Crime Science*, 9(14), https://doi.org/10.1186/s40163-020-00123-8.

Cerulus, L. (2021) One group that's embraced AI: Criminals, *Politico*, available at: https://www.politico.eu/article/artificial-intelligence-criminals/ (January 15, 2022).

Chigada, J. & Madzinga, R. (2021) Cyberattacks and threats during COVID-19: A systematic literature review, *South African Journal of Information Management*, 23(1), pp. 1-11, https://doi.org/10.4102/sajim.v23i1.1277.

Collier, B., Jones, R., Horgan, S. & Shepherd, L. (2020) The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations, *The Scottish Institute for Policing Research*, (1), pp. 1-18.

Coman, I. & Mihai, J.-C. (2021) The Impact of COVID-19 on Cybercrime and Cyberthreaths, *European Law Enforcement Research Bulletin*, SCE 5, pp. 61-67, available at: https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/489 (January 15, 2022).

ENISA (2021) *Countering SIM-Swapping: Overview and good practices to reduce the impact of SIM-Swapping Attacks* (Athens: ENISA).

European Commission (2021a) *Fighting disinformation*, available at: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation_en (January 15, 2022).

European Commission (2021b) *The Digital Economy and Society Index (DESI)* (11), available at: https://digital-strategy.ec.europa.eu/en/policies/desi (January 15, 2022).

Europol (2014) *Internet Organised Crime Threat Assesment (IOCTA)*, available at: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (January 15, 2022).

Europol (2021) *Internet Organised Crime Threat Assesment (IOCTA)*, available at: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (January 15, 2022).

High, P. (2020) Who Led Your Digital Transformation? Your CIO Or COVID-19?, *Forbes* (May 26, 2020), available at: https://www.forbes.com/sites/peterhigh/2020/05/26/who-led-your-digital-transformation-your-cio-or-covid-19/ (January 15, 2022).

Hoffman, I. (2021) Cybersecurity and public administration in the time of corona(virus) – in the light of the recent Hungarian challenges, *Cybersecurity and Law*, 3(1), pp. 145-158.

Horváth, Cs. L. (2021) A Hungarian family's bank account was zeroed out in a criminal fraud, *24.hu*, available at: https://bit.ly/3eRqr8H (January 15, 2022).

Hungarian Central Statistical Office (2019) Educational data, 2019/2020 (preliminary data), *Statisztikai Tükör*, available at: www.ksh.hu (January 15, 2022).

Kemp, S. (2021) Digital 2021: Global Overview Report, *DataReportal*, available at: https://datareportal.com/reports/digital-2021-global-overview-report (January 15, 2022).

Kirchengast, T. (2020) Deepfakes and image manipulation: criminalisation and control, *Information & Communications Technology Law*, 29(3), pp. 308-323, https://doi.org/10.1080/13600834.2020.1794615.

Lalliea, H. S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. (2021) Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, *Computers & Security*, 105, pp. 1-13, https://doi.org/10.1016/j.cose.2021.102248.

Marczak, B., Scott-Railton, J., Razzak, B.A., Al-Jizawi, N., Anstis, S., Berdan, K. & Deibert R. (2021) NSO Group iMessage Zero-Click Exploit Captured in the Wild, *The Citizen Lab*, available at: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/ (January 15, 2022).

Murrar, F. (2021) Fraud schemes during COVID-19: a comparison from FATF countries, *Journal of Financial Crime*, 29(2), pp. 533-540, https://doi.org/10.1108/JFC-09-2021-0203.

National Cyber Security Center (2021) *Alert on sms messages related to the distribution of malicious code that misuse the name of parcel service providers*, available at: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/ (January 15, 2022).

NMHH (2021) "*SIM card replacement made safer*", available at: https://nmhh.hu/cikk/223395/NMHH_biztonsagosabba_valt_a_SIMkartyak_csereje (January 15, 2022).

Palicz, T., Bencsik, B. & Szócska, M. (2021) Kiberbiztonság a koronavírus idején – a COVID-19 nemzetbiztonsági aspektusai [Cybersecurity in the age of the coronavirus - national security aspects of COVID-19], *Scientia et Securitas*, 2(1), pp. 84-85.

Prosecutor's Office of Hungary (2020) *The court arrested the fraudsters who sold masks* (April 3, 2020), available at: https://ugyeszseg.hu/a-birosag-letartoztatta-a-szajmaszkokkal-uzletelo-csalokat/ (January 15, 2022).

The White House (2021) *Background Press Call on the Virtual Counter-Ransomware Initiative Meeting*, available at: https://www.whitehouse.gov/briefing-room/press-briefings/2021/10/13/background-press-call-on-the-virtual-counter-ransomware-initiative-meeting/ (January 15, 2022).

Tidy, J. (2020) Google blocking 18m coronavirus scam emails every day, *BBC News*, available at: https://www.bbc.com/news/technology-52319093 (January 15, 2022).

U.S. Department of Justice (2018) *Report of the Attorney General's Cyber Digital Task Force* (Washington: DoJ).

Wall, D. (2021) The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending, *European Law Enforcement Research Bulletin*, SCE 5, Special Conference Edition Nr. 5, pp. 45-60.

Wan Fei Ma, K. & McKinnon, T. (2021) COVID-19 and cyber fraud: emerging threats during the pandemic, *Journal of Financial Crime*, 29(2), pp. 433-446, https://doi.org/10.1108/JFC-01-2021-0016.

Whyte, C. (2020) Deepfake news: AI-enabled disinformation as a multi-level public policy challenge, *Journal of Cyber Policy*, 5(2), pp. 199-217, https://doi.org/10.1080/23738871.2020.1797135.

Cybersecurity of the Hungarian Municipal Administration: Challenges of a Fragmented System

ISTVÁN HOFFMAN

Abstract In this chapter the situation and the challenges on the cybersecurity issues of e-administration services and practice of Hungarian municipalities will be analysed. However, the cybersecurity of the municipal administration became an important part of the local decision-making and administration in Hungary, it has several challenges because of the fragmented Hungarian municipal system. The regulation on local cybersecurity issues focused on the development a horizontally integrated e-administration. Although the acts on this system have been passed in the last years, and the former restrictions of the electronic administration have been eliminated, but the practice of the Hungarian e-administration is partly different. The new, enhanced e-administration resulted new challenges, which was partly solved by the radical nationalisation and centralisation of the former municipally performed tasks. The municipal e-administration systems have been built mainly by the largest municipalities, but their operation could be further developed, and thus the municipal cybersecurity is a developing part of the Hungarian public administration tasks, as well.

Keywords: • digitalization • e-administration • cybersecurity • Hungary • digitalization of municipal authorities • municipal administration

CORRESPONDENCE ADDRESS: István Hoffman, Ph.D., Prof. Dr. Hab., Eötvös Loránd University, Faculty of Law, Department of Administrative Law, 1053 Budapest, Egyetem tér 1-3, Hungary, e-mail: hoffman.istvan@ajk.elte.hu; Marie Curie-Skłodowska University, Faculty of Law and Administration, Department of International Public Law, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland, e-mail: i.hoffman@poczta.umcs.lublin.pl; Senior Research Fellow, Centre for Social Sciences, Institute for Legal Studies, 1097 Budapest, Tóth Kálmán u. 2-4, Hungary, e-mail: hoffman.istvan@tk.mta.hu.

https://doi.org/10.4335/2022.2.16 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Today, the digital revolution has also caught up with the administration. E-governance has many advantages. For example, clients are not tied to office hours, do not have to meet with officers, they can access information more easily, and many tools are available to help them make decisions (Bowman & Kearney, 2016: 223). The *e-government* is an umbrella term: it covers the government innovation and the government information and services – according to the relevant literature. The aim of e-government is often referred as the paperless office, which means that electronic administration converts paper processes into electronic processes. E-government creates a lot of ways that in governments and citizens can communicate with each other. As a result, clients become the actors of the administrative system (Wohlers, 2010: 89-90).

The e-administration and e-government has not only benefit, but it has several risks. During the e-administration sensitive data are used and stored by the administrative bodies, and the sensitive data of the administrative decision-making can be used for these activities. Therefore, it became a major issue to defend the data and information on the citizens of a given administrative unit and the defence of the data and information on the given administrative body. Cybersecurity became an important element of the digitalisation of the public administrations (Fuster & Jasmontaite, 2020: 107).

Cybersecurity and e-government has another important questions: the smart cities and the platforms of the municipal administrations and services are mainly based on and are backed up by the centralised government data banks and systems, and the accessibility to the date of these systems are regulated centrally. Therefore, there is a challenge of a new type of centralisation which will be even examined by this paper.

Municipal e-administration have an important issue in the last two years: the COVID-19 pandemic has been an opportunity, a challenge, and a threat for the local public administrations, especially for the local e-administration. The application of the e-administration has been strengthened by the reduction of the contacts between persons. Therefore, the tools and institutions of e-administration has been widely used by the administrations during the time of pandemic. The application of the e-administration could be interpreted not only as a challenge and opportunity to build a more effective administration, but it has only several risks, as well. The cybersecurity issues of the different administrative systems have become a recent question, as well. These trends can be observed in Hungary. As it can be seen, the Hungarian administrative law had diversified and detailed regulation on e-administration, but the extended application of the tools and institutions of e-administration has had several – especially in the field of cybersecurity.

This chapter focuses on the challenges of the municipal administration in the field of the cybersecurity, especially the role of the municipalities as authorities. The central elements

of the review are the analysis of the legal regulation on (municipal) e-Government e-Administration and cybersecurity and secondly the review of the digitalisation of the Hungarian municipalities and especially their responsibilities in the field of the defence against cyber-attacks.

2 Methods

First of all, the analysis is based on the methods of the *jurisprudence*. Therefore, firstly the concept and the legal regulation on the digitalisation of the administrative services will be reviewed, especially the services provided by Hungarian municipalities. As part of this analysis the basic elements of the concept of the e-administrative services will be shortly shown. After that I would like to analyse the framework of the regulation on cybersecurity in the Hungarian municipalities.

The expectations – the legal regulation – and the reality could be compared. Not only the legal regulation has been analysed but I tried to show the framework of the Hungarian challenges, the recent situation of the Hungarian municipal administration and the link between this situation and the cybersecurity challenges.

3 The analysis of the regulation on the eGovernment and its cybersecurity issues in Hungary

Firstly, I would like to examine the analysis of the regulation on eGovernment, especially on the e-tools of the authorities in Hungary. After this analysis we would like to review the actual situation of the e-administration in the large Hungarian municipalities. But as a preliminary issue, we would like to analyse the interpretation of the e-services, especially the e-services of the Hungarian municipal administration.

4 Municipal e-administrative services

The e-services are different, and the different stages of e-administration is distinguished. Four main stages of the e-government development are distinguished. This classification is based on the integration of the different services and on the complexity of the structures and technology. The first stage is the *catalogue,* in which the online presence of the government is provided, the main tasks are catalogued, and the several forms could be downloaded. The second stage is the *transaction,* in which the services and forms are online, and the online transactions are supported by several working databases. The third stage is the *vertical integration,* in which the local systems are linked to higher systems (within similar functionalities). The fourth stage is the *horizontal integration,* in which the systems with different functions are integrated and a real one-stop-shop is provided (Layne, 2001: 124-125).

It is highlighted by the literature, that significant investments are required to fulfil these aims, and the costs of these investments are partly related to the cybersecurity issues (Heeks, 2006: 107 and Légárd, 2020: 92). But the e-government technologies have several prerequisites. After Layne and Lee three vital condition should be fulfilled to implement a successful e-government reform: universal access to the e-government tools, the defence of privacy and confidentiality and – last but not least – the citizen focus in government management (Layne, 2001: 134 and Chałubińska-Jentkiewicz, 2021: 178-181).

5 Municipal e-administration in Hungary - a short review

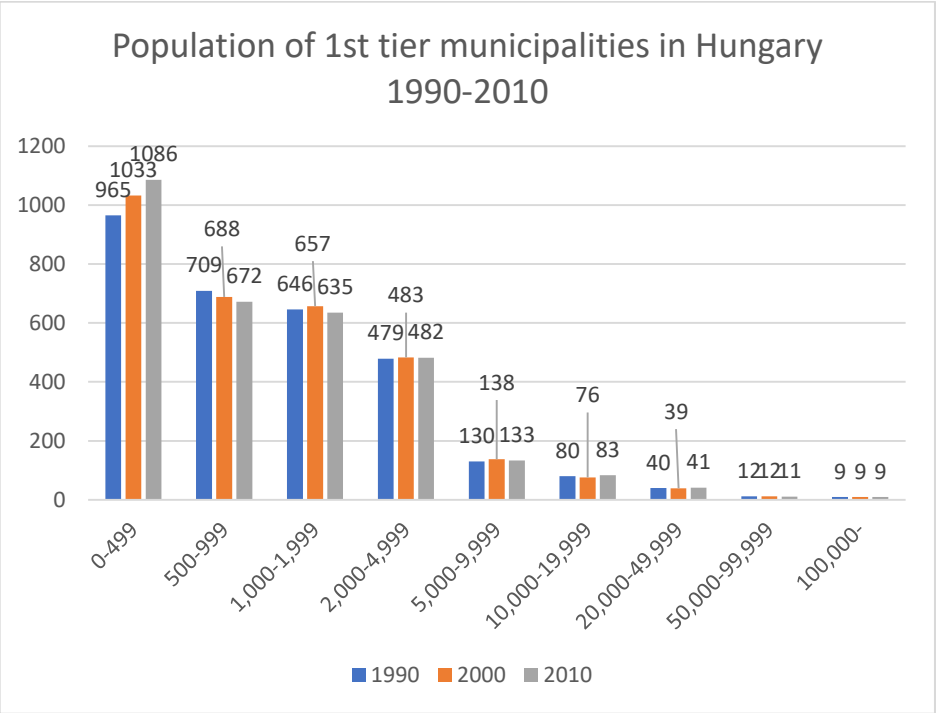
The Hungarian public administrative system was a highly decentralised one before the reforms of 2011/2013. After the Democratic Transition a very fragmented and very autonomous municipal system evolved.

Table 1: Population of the Hungarian municipalities (1990-2010)

Year	0-499	500-999	1,000-1,999	2,000-4,999	5,000-9,999	10,000-19,999	20,000-49,999	50,000-99,999	100,000-	All
	Inhabitants									
1990	965	709	646	479	130	80	40	12	9	3,070
2000	1,033	688	657	483	138	76	39	12	9	3,135
2010	1,086	672	635	482	133	83	41	11	9	3,152

Source: Szigeti, 2013: 282.

Figure 1: Population of the Hungarian municipalities (1990-2010)



Source: Szigeti, 2013: 282.

The majority of the tasks of the local authorities belonged to the competences of the local bodies especially as delegated administrative tasks of the officers of the Hungarian municipalities. Therefore, the general first instance body of the Hungarian public administration was the municipal clerk before 2010 (Fábián & Hoffman, 2014: 330). Therefore the eGovernment issue of the Hungarian local government system became a significant element of the Hungarian strategies and service provision.

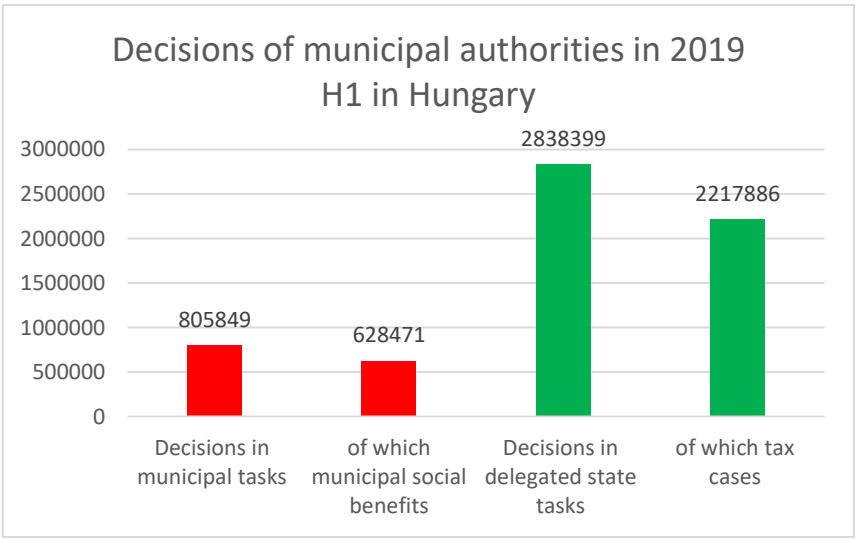
In Hungary the development of the municipal e-administration was partly a 'from bottom to top' initiatives, especially in the large municipalities, but it is highlighted, that primarily the local e-administration was a top-bottom initiative (Hoffman & Cseh, 2020: 199-211). Now a unified government portal has been organised and the local (municipal) systems are integrated in it.

The evolvement of the municipal eGovernment system begun at the end of the 20th century. Several problems have been occurred: firstly, the general administrative knowledge of the citizens and the accessibility to the e-tools were limited. Therefore –

and because of the limited form a bottom to the top approach – the online presence of the larger municipalities were provided in the early 21st century. As it will be reviewed later, the Act XC of 2005 on the freedom of electronic information was a turning point. New platforms were developed in this time, firstly in several sectors (for example in the municipal finances, later in the field of construction administration). An integrated national system has been developed after the Millennia, the www.magyarorszag.hu site and the Government Portal and its Client Gate. Originally the municipalities were not fully integrated, but the tendency of integration has been strengthened. After the reforms of 2010 the integration of the local and central was an important reforms issue (Budai, 2013: 134). A new model of the municipal e-administration was evolved after the amendment of the administrative and tax procedural acts, because the municipalities should provide fully electronic administrative platform in the field of local taxes.

After 2010 the recentralisation and the concentration of the public administration can be observed in Hungary. Till 2013 the municipal clerks were the major 1st tier authorities in the Hungarian system of the public authorities, but it changed by the establishment of the district offices of the county government offices and by the transfer of the competences to the district and county offices from these municipal officers (who performed state administration). However, the municipal clerks perform significant competences, but it should be highlighted, that the majority of the municipal decisions belongs to the delegated state-tasks (which are actually central tasks, but because of the grassroot administration they are performed by local – municipal – bodies).

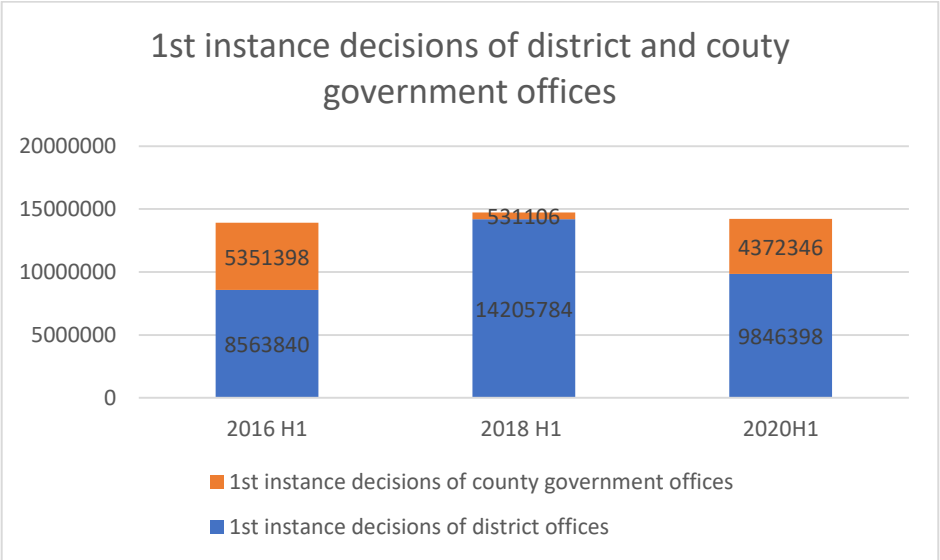
Figure 2: Decisions of municipal bodies in Hungary



Source: OSAP, 2020.

Therefore, the fragmented local administrative structure has been a challenge to the Hungarian public administration system. As we have mentioned, one answer was the centralisation of the competences to the district and county government offices. Now, the major 1st instance authorities are these bodies, as it can be seen at the Figure 3.

Figure 3: 1st instance cases of the district and county government offices



Source: OSAP, 2020.

The second answer of the administrative reforms to the fragmentation of the municipal system was the concentration of the competences. The new Act on the Local Self-Government of Hungary (Act CLXXXIX of 2011) stated, that joint municipal offices shall be established by the small municipalities (municipalities which have less than 2000 inhabitants). Thus, the main form of the rural local administration became the joint municipal offices (see Table 2).

Table 2: Joint municipal offices and independent municipal offices in Hungary (2020)

Number of municipalities in Hungary	Independent municipal offices	joint municipal offices	Number of participant municipalities
3 153	521	749	2632

Source: KSH, 2020.

These transformations impacted the municipal e-services and the cybersecurity issues of them.

6 The legal framework of eGovernment in Hungary

It is a main strategic goal for Hungary to modernize its public administration. The goal is to increase the use of modern information and communication technologies in the communication between state institutions themselves and between state institutions and citizens. During the last few years, considerable measures have been taken by the Hungarian government to reform the public administration of the country. The most important results of these reforms include the reduction of administrative burdens and the simplification of administrative procedures.

From October of 2009 (with Act CXI of 2008) the general administrative procedure rules were amended. Electronic communication between clients and authority became available through the use of an online citizen portal dedicated to this end, called Client Gateway.

In April 2012, with the amendment of the Act CXL of 2004 on the General Rules of Administrative Procedures and Services by the Act CLXXIV of 2011, and the introduction of the so-called regulated electronic administration services, the legal preconditions for eGovernment services were established (Baranyi, 2013: 222-225). In addition to this, in July 2015 a new law on the Hungarian eID card has been adopted.

As the scope of the Hungarian eGovernment developments continuously grew, the need for a separate eGovernment law appeared. Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions (hereinafter referred to as ET Act) kept the achievements of the 2012 reform and further extended the possibilities of electronization of processes.

As of January 2018, a new act regulating administrative procedure entered into force (Act CL of 2016 on the Code of General Administrative Procedure). In Section 26, the new act also regulates the communication of the authorities with clients and utilise the electronic communication means provided by the ET Act as a form of written communication. (It is also allowing electronic communication not in accordance with the ET Act, but that is regarded as oral communication.) The new Procedure Act, according to its general concept, is not containing detailed rules of this form of communication but rely entirely on the ET Act. There is also an option to deliver the decision by the ET Act, in place of an official document, regulated in Subsection 3 of Section 85 (Baranyi, 2017: 317-319).

According to the ET Act, it is mandatory for municipal governments to provide the option for electronic communication for clients. To be precise, it is mandatory for almost

all governmental bodies to provide this option. There are only few exception to this rule: when an act or government decree adopted in a vested legislative capacity creates an obligation for the physical presence of the client, or for the submission of documents that may not be obtained in any other way; where it is not applicable; when it contains classified information or when it is excluded by an international treaty or a directly applicable Community legislation that is binding in its entirety (Section 8 of the ET Act).

Clients shall have the option to make statements, take procedural steps and fulfil other obligations either through a single, personalized communication interface or through e-governance services platform if it is provided (Section 10 of the ET Act).

The ET Act contains the general rules of the electronic connection between the body providing e-governance services and the client, as well as the provisions on the IT cooperation between the body providing e-governance services and other bodies. An important provision for local authorities is provided in ET Act. According to Section 1 17. b), local authorities are bodies providing e-governance services which are obliged to ensure electronic administration services as specified in the ET Act from 1 January 2018. ET Act Section 9 (1) paragraph a) and b) also states that electronic communication is mandatory for economic operators acting as clients and for the legal counsels of clients from 1 January 2018. There is an obligation to maintain electronic communication, then any statement not in compliance with this regulation shall be deemed invalid. The only exception under this regulation is when the client can't maintain electronic communication due to a failure of the system on behalf of the authority, when the electronic administration service cannot be accessed or when the required forms can't be reached because of it wasn't provided.

For clients, ET Act does not make electronic communication mandatory but it gives them the opportunity to use this form of communication.

In general, it can be said that in any type of cases local authorities provide the electronic administration services for their clients via electronic form services on their websites or in other cases through e-Paper services. In cases in which it is not possible to use electronic forms, clients are required to use the e-Paper services. In most cases, the electronic form services can be used through Client Gateway, which is the most widely used and most essential eGovernment application in Hungary.

E-Paper is a general purpose electronic application form, a free, authenticated messaging application that connects clients electronically with the institutions and bodies connected to the service via the Internet. The purpose of the e-Paper service is to enable the client to submit a complaint to the authority electronically for those procedures or simple matters which are not supported by a system of expertise for their frequency or other reasons. The e-Paper service is available through Central Identification Agent, at https://epapir.gov.hu.

The public services are another important issue of the cybersecurity of the local administration. These – mainly human – public services have been widely centralised in Hungary during the 2010s, thus the Another important formerly municipally managed public education, health care, residential social and child care and several cultural services are now provided by institutions which are mainly maintained by the central administration and by its territorial agencies (Hoffman et al., 2016: 462-467). Therefore, new platforms have been evolved, which provide information and data for the service provision, as well for financing these services. Such an e-platform for the public education is the *KRÉTA* system, for the health care services the *EESZT (Elektronikus Egészségügyi Szolgáltató Tér – Electronic Health Care Provision Space)* and the unified social register. The providers – which are maintained mainly by the agencies of the central administration, however there are municipal maintainers and the churches and NGOs have maintainer tasks, as well – have direct connection to these systems. The major elements of these platforms are regulated by Act of Parliaments and the executive decrees issued by the Government of Hungary.

As we have mentioned earlier, this process requires significant human and financial resources. The digitalisation and the eGovernment investments and reforms in Hungary– as an element of the economic and regional development – is co-funded by the European Union. The support of the digital and e-administration is an important objective of the operational programme supporting the development of the Hungarian public administration and public services (Közigazgatás-és Közszolgáltatás-fejlesztési Operatív Program – KÖFOP). The municipal e-administration projects are funded by this programme, as well.

7 Transformation of the legal framework of the municipal e-administration

There is also an online system, called The Local Government Office Portal (hereafter referred to as Portal) which is the location of the e-government administration in the local ASP system. The Portal provides municipalities with a local government ASP system for both natural persons and legal entities, providing the opportunity to use electronically available services for specialist applications.

Through the Portal, the clients can query for a local tax balance, the status of local government affairs electronically initiated by the Portal. They can also initiate an administrative action using it. At present, the local government's tax, industrial, commercial, estate inventory, estate protection, birth and social affairs are supported by system development through the local ASP system. The application provides customers with the opportunity to track the process of their administrative procedures over the Internet. The Portal is mostly used by smaller municipalities, bigger cities both with and without county rights (which are the scope of this paper) normally use their own websites.

Another important field of the municipal e-administration is the *Smart City* programs. Although the welfare and cultural services are significant element of the Smart City services in the majority of the developed countries (Lytra & Visvizi, 2018: 2000-2006), the Hungarian regimes do not follow the international patterns (Henk, 2018: 231-237). The main reason of the different Hungarian pattern is that the majority of the welfare and educational services were nationalised and centralised between 2011 and 2016 therefore, the role of the municipal administration is limited in these sectors. Secondly, the 'customers' of these services have interest in smart solutions. This attitude has been amended during the COVID-19 pandemic and the regular use of the health platforms have been increased (Hoffman, 2021: 152-153). The approach of smart city is based on the role of the ICT technologies as a platform of the more efficient local service provision. One of the major fields of the smart city solutions is the *local transportation.* First of all, new platforms for the provision of public transport services were introduced by the larger Hungarian municipalities. Such a unified public transport platform is the BKK FUTÁR in Budapest, which allows to control and to observe the public transport services of the Budapest Transport Company. Secondly, the street parking has been reformed by digital service and by new local platforms. However, these street parking platforms were developed by the municipalities, but they have direct link to the centralised Hungarian national mobile payment system, therefore, it is partially centralised.

As I have mentioned earlier, the municipal platforms can be interpreted as a tool for the 'soft' or 'latent' centralisation. These local systems are mainly based on data provided by the centralised databank and platforms. Therefore, the access to these central systems is a crucial element of the operation of these local systems. Because the access to these data are managed by the central systems therefore, the operation of the local systems are partially determined by the central system and by the access to them. Thus, the central government can influence and impact the local service provision. This impact can be interpreted as a soft one, because the impact is not direct, it is based on the use of the centralised databanks and on the architecture of these central regimes.

8 Cybersecurity issues and municipalities in Hungary

Cybersecurity became an important issue of the municipal administration after the Millennials, especially after 2010, when the eGovernment and the municipal e-services begun to evolve rapidly. Thus, cybersecurity became part of the public order and safety policies of the Hungarian administrative system. This transformation has been similar to the changes of other Visegrád Countries (Karpiuk, 2019: 30 and Czuryk & Kostrubiec, 2019: 34-36).

After the challenges of the new era, especially to ensure a better defence of the administrative cyberspace, a new regulatory approach has been evolved after 2010. A general act on the cybersecurity of the central and local government bodies was passed in 2013. This framework act, the Act L of 2013 on the cybersecurity of state and municipal

bodies (hereinafter: CSA) follows the major principle of cybersecurity regulations. It is based on the 'CIA' principle; thus confidentiality, integrity and availability shall be secured by the cybersecurity activities. Security classes and measures are defined by the Act; however, the detailed regulation can be found in an implementing ministerial decree. Following the general approach, the tiers of cybersecurity defence are defined and regulated by the CSA. The Act follows the general regulation, and especially, because its scope is a very wide one, and even the Hungarian military forces are affected, it follows the NATO regulations as well, not only the EU rules (because of the Hungarian NATO-membership).

A centrally supervised system has been regulated: the major body responsible for cybersecurity issues is in Hungary the Ministry of Interior, because cybersecurity is interpreted in Hungary as mainly a public order and security issue, the military elements are important, but a general regulation has been established. The central body of the cybersecurity issues is one of the national security agencies (which are supervised by the Minister of Interior), by the Special Service for National Security (Juhász et al., 2020: 136-138).

9 Challenges of the municipal cybersecurity in Hungary

The Hungarian regulation – including the CSA – fit the strict and detailed European and NATO requirements. Thus, the major challenges of the municipal cybersecurity are linked to these requirements. As we have mentioned earlier, in Hungary there are more than 3000 municipalities (for a population which is less than 10 million inhabitants) and there are 1270 independent municipal offices, whose majority are relatively small offices (typically they have less than 20 civil servants). These offices have often lack of resources and lack of human capacities, especially in the field of cybersecurity. Because of the existence of delegated state tasks, these municipalities have links to the central systems, especially to the registrations of the population and their addresses. Therefore, these small offices can be an Achilles heel of the Hungarian system, because they are more vulnerable than the national(ised) systems.

Even the larger municipalities have significant cybersecurity issues: the local platforms and their links to the centralised system can be even vulnerable, and it is important to protect them. However, the centralised protection of these systems can be even interpreted as a new model and soft centralisation of the service provision.

10 Conclusions

The digitalisation and the e-administration are important issues of the public administration reforms of the last decades. The challenges of the new, digital ages resulted the transformation of the traditional administration. As we reviewed, the Hungarian regulation on eGovernment and on the digitalisation of the public administration

transformed significantly. The regulation was focused on the development a horizontally integrated e-administration. The practice of the Hungarian e-administration is partly different. The municipal e-administration systems have been built by the municipalities (especially by the larger municipalities), but their operation could be developed. The fragmented municipal system and their links to the national systems could be a vulnerable element of the Hungarian cybersecurity system, however, the regulation and the supervision activities are detailed regulated and have evolved quickly during the last years. However, the centralised systems and their centralised protection can be interpreted as a new model centralisation, because the local service provision are influenced by these national systems.

References:

Bowman, A. O' M. & Kearney, R. (2016) *State and Local Government* (Boston: Cengage Learning).

Baranyi, B. (2013) A kapcsolattartás általános szabályai, In: Barabás, G., Baranyi, B. &. Kovács, A. Gy (eds.) *Nagykommentár a közigazgatási eljárási törvényhez* (Budapest: CompLex), pp. 217-234.

Baranyi, B. (2017) Az elektronikus ügyintézés szabályai, In: Fazekas, M. (ed.) *Közigazgatási jog. Általános rész III* (Budapest: ELTE Eötvös), pp. 311-322.

Budai, B. B. (2013) *Az e-közigazgatás elmélete* (Budapest: Akadémiai Kiadó).

Chałubińska-Jentkiewicz, K. (2021) Access to the ICT Network as a Public Task of Local Government, *Lex localis – Journal of Local Self-governments*, 19(1), pp. 175-195, http://doi.org/10.4335/19.1.175-195(2021).

Czuryk, M. & Kostrubiec, J. (2019) The legal status of local self-government in the feld of public security, *Acta Universitatis Wratislaviensis Studia nad Autorytaryzmem i Totalitaryzmem*, 41(1), pp. 33-47, http://doi.org/10.19195/2300-7249.41.1.3.

Fábián, A. & Hoffman, I. (2014) Local self-governments, In: Patyi, A. & Rixer, Á. (eds.) *Hungarian Public Administration and Administrative Law* (Passau: Schenk Verlag), pp. 320-349.

González Fuster, G. & Jasmontaite, L. (2020) Cybersecurity, Regulation in the European Union: The Digital, the Critical and Fundamental Rights, In: Christensen, M., Gordijn, B. & Loi, M. (eds.) *The Ethics of Cybersecurity* (Cham: Springer Nature), pp. 97-119, http://doi.org/10.1007/978-3-030-29053-5_5.

Heeks, R. (2006) *Implementing and Managing E-Government* (London: SAGE).

Tamás, H. (2018) Okosváros-megoldások Magyarországon, In: Gyula, S. (ed.) *Az okos város (Smart City)* (Budapest: Dialóg Campus), pp. 217-240.

Hoffman, I. & Cseh, K. B. (2020) E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary, *Cybersecurity and Law*, 2(2), pp. 199-211.

Hoffman, I. (2021) Cybersecurity and public administration in the time of corona(virus) – in the light of the recent Hungarian challenges [Cyberbezpieczeństwo a administracja publiczna w czasah koronawirusa w odniesieniu do niedawnych wyzwań na Węgrzech], *Cybersecurity and Law*, 3(1), pp. 145-158.

Juhász, Z., Virányi, G., Hegedűs, T. & Visztra, T. (2020) A Nemzetbiztonsági Szakszolgálat hatósági feladatai, *Nemzetbiztonsági Szemle*, 8(1), pp. 126-147, http://doi.org/10.32561/nsz.2020.1.8.

Karpiuk, M. (2019) Position of the Local Government of Commune Level in the Space of Security and Public Order, *Studia Iuridica Lublinensia*, 28(2), pp. 27-39, http://doi.org/10.17951/sil.2019.28.2.27-39.

KSH (2020) *Hungarian Central Statistical office*, available at: www.ksh.hu (December 18, 2021).

Layne, K. & Lee, J. (2001) Developing fully functional E-government: A four-stage model, *Government Information Quaterly*, 18(2), pp. 122-136, http://doi.org/10.1016/S0740-624X(01)00066-1.

Lytras, M. D. & Visvizi, A. (2018) Who Uses Smart City Services and What to Make of It: Toward Interdisciplinary Smart Cities Research, *Sustainabilty*, 10(6), pp. 1998-2013, http://doi.org/10.3390/su10061998.

Légárd, I. (2020) Te is célpont vagy! – A közszolgálat felkészítése a kiberfenyegetésekre, *Hadmérnök*, 15(1), pp. 91-105, http://doi.org/10.32567/hm.2020.1.7.

OSAP (2020) *Hatósági statisztika – OSAP adatgyűjtés alapján*, available at: www.kormany.hu/hu/dok?page=10&source=7&type=308#!DocumentBrowse (December 18, 2021).

Szigeti, E. (2013) A közigazgatás területi változásai, In: Horváth, T. M. (ed.) *Kilengések. Közszolgáltatási változások* (Budapest: Pécs), pp. 269-290.

Tomlinson, R. (2019) The failure to learn from others: Vertical fiscal imbalance, centralisation and Australia's metropolitan knowledge deficit, *Austrialian Journal of Public Administration*, 78(2), pp. 213-226, http://doi.org/10.1111/1467-8500.12387.

Wohlers, T. E. (2010) Local E-Government Sophistication in the United States, In: Scholl, H. J. (ed.) *E-Government: Information, Technology and Transformation* (London, New York: Routledge), pp. 89-106.

Authorities Competent for Cybersecurity in Germany

AGNIESZKA BRZOSTEK

Abstract In Germany, the federal states are generally responsible for the prevention of threats in cyberspace. The Federal Government has special jurisdiction over threat prevention in certain areas, such as international terrorism, security in the territory belonging to the federal railways, border protection, and national self-protection, where jurisdiction extends to the cyber domain. Cooperation between the Federal Government and Länders is essential. Germany's new Cybersecurity Strategy, adopted by the Federal Government on 8 September 2021, provides a framework for government action for the next five years. Germany was one of the first countries to respond to cyber threats in Europe. The Strategy announced the setting up of an institution, within the remit of the Federal Ministry of the Interior, whose task would be to provide technical support to federal security and technical authorities, including intelligence services, in their operational cyber capabilities. The German Federal Government's cybersecurity policy is consistent and in line with the European Union's cybersecurity policy. The multiplicity of tasks requires the involvement of multiple actors who, in a decentralised form, carry out tasks at both strategic and operational levels.

Keywords: • Germany • cybersecurity strategy • critical infrastructure • federal government

CORRESPONDENCE ADDRESS: Agnieszka Brzostek, Ph.D., Lecturer, War Studies University in Warsaw, Institute of Law, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: brzostek.agnieszka@gmail.com.

https://doi.org/10.4335/2022.2.17 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

Germany's new Cybersecurity Strategy, adopted by the Federal Government on 8 September 2021, provides a framework for government action for the next five years. The Strategy is in line with the European Union's cybersecurity policy. The NIS Directive (EU 2016/1148) requires Member States to create a steering framework in the Strategy, to identify objectives and priorities, and to designate the authorities that will be responsible for achieving these objectives. The effective implementation of the Strategy requires the adoption of legal and organisational solutions. Hence, the purpose of this paper is to analyse the legal and administrative forms of action of the federal authorities established for the implementation of cybersecurity tasks. An issue of major importance is the legal and formal way of organising the system that would take into consideration the form of action of the authorities.

It should be noted that Germany was one of the first countries to respond to cyber threats in Europe. As pointed out in 2005, cybersecurity must be part of national security. In 2011, the government adopted its first Cybersecurity Strategy (The 2011 Strategy, p. 3-4). According to C. Guitton, Germany adopted the Cybersecurity Strategy as a form of preventive policy, unsupported by any incidents concerning critical information infrastructure. The level of threat was significantly influenced by unverifiable data supplied by cybersecurity providers and the impact which events taking place in other countries had on them, e.g., in the USA (C. Guitton, p.22). The adoption of the Strategy resulted in establishing the National Cybersecurity Council, whose task was to oversee the implementation of the Strategy's objectives and, if necessary, to adapt strategies and measures to the specific requirements and framework conditions arising from it (The 2011 Strategy, p. 7). In 2011, the Ministry of the Interior of the Federal Republic of Germany set up the National Cyber Response Centre (Nationale Cyber-Abwehrzentrum – NCAZ), which was supposed to become the first link in the fight against cyber threats and to provide a platform for cooperation between the competent authorities of the German administration. The Germans decided not to institutionalise the work of the Centre due to the order for the separation (*Trennungsgebot*) of special services from police services (Sacewicz, pp. 129-130). Currently, the Centre consists of the following bodies the Federal Office for Military Counterintelligence, the Federal Criminal Police Office, the Federal Office for Information Security (*BSI – Bundesamt für Sicherheit in der Informationstechnik*), the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz – BfV*); the Federal Office of Civil Protection and Disaster Assistance (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK*); the Federal Criminal Police Office (*Bundeskriminalamt – BKA*); the Federal Intelligence Service *(Bundesnachrichtendienst – BND*); the Federal Police (*Bundespolizei – BPol*), and the cyberspace and information space of the Command of Bundeswehr (the armed forces of the Federal Republic of Germany). Included as external partners are the Bavarian Cyber Defence, cyber specialist prosecutors from Bamberg and Cologne and the Federal Financial Supervisory Authority.

The most important tasks of the Centre include preventing and combating threats in cyberspace, which includes exchanging information, analysing and evaluating

information incidents, developing mechanisms for the effective protection, preventing and neutralising the outcomes of attacks, as well as assessing the effectiveness of the implementation of the cyberspace protection strategy. The Centre's affiliated authorities provide information according to their competence – the BSI evaluates incidents in technical terms, the BfV investigates whether a foreign special service is responsible for an attack, and the BBK assesses the effects of attacks on critical infrastructure. The other authorities identify new attack methods and tools. As a result, the NCAZ can provide, within a short period of time, up-to-date and comprehensive information on threats against cyberspace. As part of preventive measures, the NCAZ periodically, and additionally when necessary, provides the National Cybersecurity Council with relevant guidelines, and in emergency situations reports directly to the crisis management centre at the Ministry of the Interior (Sacewicz, pp. 129-130, Oleksiewicz, pp. 47-51).

The assumptions adopted in the Strategy for the activities of the authorities were criticised by experts. It was argued that the composition of the National Cybersecurity Council was indicated in a manner that was too general. As noted in a confidential report prepared by the Federal Office for Control, the Council is not an appropriate institution for repelling an attack because it does not have a sufficient number of staff and its area of activity is not clearly defined (S. Steller, pp. 52-53). There were also expert opinions that Germany's involvement in foreign cooperation, as indicated in the Strategy, should be described more precisely and in more detail, i.e., how exactly this cooperation should look (Steller, p. 53).

Germany's Cybersecurity Strategy adopted in 2016 identified the need to build a sustainable cybersecurity system (The 2016 Strategy, p. 9). The National Cyber Response Centre (NCAZ) organised its structure at the federal level in such a way that the various actors could cooperate in their activities. An important objective was to intensify cooperation with Länders (federal states) and to make them more involved. As part of the NCAZ, the federal authorities responsible for cybersecurity issues exchange information on cyber incidents in the Cyber-AZ and share their assessments and analyses. In order to strengthen cyber defence capabilities, the Cyber-AZ has been appropriately configured and organisationally strengthened within a nationwide cybersecurity architecture, and as a departmental institution it will develop into a central platform for cooperation and coordination under the directorship of the Federal Ministry of the Interior (the 2016 Strategy, pp. 27-28).

The implementation of the NIS Directive in Germany required legislative changes. The Implementing Act to the NIS Directive of June 2017 established the basis for setting up Mobile Incident Response Teams (MIRTs) at the BSI. Meanwhile, options for detecting and blocking cyber-attacks were broadened in telecommunications law. Mobile Incident Response Teams (MIRTs) were established at the BSI to analyse and clear up cyber incidents in institutions. Upon the request of the MIRT, the BSI will be able to provide support to constitutional authorities, federal authorities and operators of critical infrastructures, as well as similarly important institutions. This assistance is intended to

rapidly restore the safe technical operations of the institutions concerned (The 2016 Strategy, p. 29). A specific feature of the German solution is that the BSI is entrusted with control over how to implement detailed protection procedures in those departments of critical infrastructure that determine the way society functions. The following systems have been identified as such: banking, energy, water supply (drinking water delivery), food, telecommunications and information technology. As the tasks refer to the operators of ICT networks and institutions using them in terms of data protection, forms of security in case of their digitisation and attempts to hack personal accounts in the system, it was decided to distribute the competences of federal institutions in this way. The BSI is authorised to implement procedures on critical infrastructure elements of information systems, whose procedures refer both to the way they are used and to the changes introduced, and investments made in order to secure their functionality (Mickiewicz, p. 76).

Cyber-attacks might also require action by local federal security agencies. To this end, the Federal Criminal Police Office (BKA) set up a specialised investigative unit, the Quick Reaction Force (QRF), which, in consultation with the responsible public prosecutor's office or the Office of the Federal Prosecutor, conducts the first criminal procedure for law enforcement agencies (The 2016 Strategy, p. 29). "Mobile Cyber Teams" were set up within the BfV itself, which are made up of IT specialists, intelligence specialists experienced in analysing cyber-attacks and, if necessary, staff with foreign language skills. These cyber teams will travel to the scene of cyber-attacks with an intelligence or extremist/terrorist background (The 2016 Strategy, p. 29).

In the defence sector, these tasks were carried out by the Military Counterintelligence Service (MAD). The Federal Intelligence Service (BND) could monitor attacks as they were being prepared and carried out. Information flows resulting from attacks are also registered. The Bundeswehr may also contribute, as much as they are allowed by the Constitution, to security preparedness with its Incident Response Teams and other relevant units. Setting up MAD is widely regarded by experts as a paradigm shift from defensive to offensive cyber defence (Bendik 2016, p. 13).

In the case of foreign intelligence services, cyber-attacks on governmental IT systems, and those of businesses, research institutes and their employees, are monitored by the BfV Directorate-General for Counterintelligence. Its scope of activity concerns cyber espionage, the evaluation of attacks on federal agencies and other targets which are thought to be the work of intelligence services. In line with its scope of activity, the BND monitors cyber spying and other cyber-attacks from abroad targeting government and/or critical infrastructures in Germany. The BND could send potential targets an early warning to take any necessary defensive action (Signals Intelligence Support to Cyber Defence (SSCD)). In this way, the BND was using IT specialists and experienced analysts to create an early-warning system for cyber-attacks (The 2016 Strategy, p. 32).

The Strategy announced the setting up of an institution, within the remit of the Federal Ministry of the Interior, whose task would be to provide technical support to federal security and technical authorities, including intelligence services, in their operational cyber capabilities. In 2017, the Centre for Information Technology of Security Authorities (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich – ZITiS*) was established. The ZITiS itself has no operational powers (The 2016 Strategy, p. 32).

In Germany, the BSI acts as the national CERT for administration and for operators of critical infrastructure, the private sector and individual users, as well as a single point of contact for foreign and international CERTs. CERTs act as computer emergency response teams, which are an important component of any sustainable cybersecurity architecture, as single points of contact for technical prevention and response in the field of IT security. There are also independent CERTs at other federal agencies and in Länders, as well as in some businesses and research institutions (The 2016 Strategy, p. 34; Mickiewicz, p. 75).

The introduction of the new Cybersecurity Strategy was preceded by the IT Security Act 2.0 adopted on 7 May 2021 (I IT-Sicherheitsgesetz 2.0). The Act essentially strengthened the competences of the BSI as the competent authority for cybersecurity. In addition to the afore-said competences, the BSI has broadened its scope of action in five key areas of activity. The first is the indication that the BSI is the national cybersecurity certification authority, pursuant to §9a (1), within the meaning of Article 58(1) of EU Regulation 2019/881. In particular, the BSI is responsible for monitoring and enforcing the provisions of law under European cybersecurity certification schemes. Another area is the detection of threats and defence against cyber-attacks. As a major competence centre for cybersecurity, the BSI can design digital security strategies by setting binding standards for federal authorities and monitoring them effectively. The next area concerns mobile network security and the certification of key components. Another area is consumer protection, which has become one of the BSI's tasks. It has become an independent consumer IT advice centre at the federal level and the authority competent for the introduction of uniform, transparent IT certification. In the area of business security, the BSI will monitor the implementation of IT security measures and the exchange of information (IT-Sicherheitsgesetz 2.0, p. 11).

The Cybersecurity Strategy was adopted by the Federal Government on 8 September 2021. The starting point of the Strategy is an assessment of the threat situation. This is marked by a considerable quantitative and qualitative increase in cyber-attacks, an expansion in the potential scope for attacks and new threat scenarios. The cybersecurity landscape includes civil society, initiatives and research institutions, business entities and governmental bodies. The objectives of the Strategy are identified in 4 areas:

1. Establishing cybersecurity as a joint task for the government, private industry, the research community and society.
2. Reinforcing the digital sovereignty of the government, private industry, the research community and society.
3. Making digital transformation secure.

4. Setting measurable and transparent objectives (The 2021 Strategy, p.6).

The presented objectives of the Strategy point to ensuring the security of citizens as the main users of IT networks. To this end, the strategic objectives envisage sensitising citizens and increasing their cyber competence. The next objective is to be achieved by strengthening, in general, cybersecurity in private industry, focusing on the protection of critical infrastructures, specifically on the operations of small and medium-sized enterprises. In this case, fostering digital sovereignty and the competitiveness of companies in the cybersecurity field is essential. Under the next objective, the following three main areas of action can be identified: 1. The distribution of competences and cooperation among the relevant authorities; 2. The enhancement of skills and powers within the authorities; and 3. New challenges facing state actors in cyberspace. As for the last objective, the Federal Government intends to achieve it through "Germany's active role in European and international cybersecurity policy" and through Germany's participation in the European Union (EU) and the North Atlantic Treaty Organization (NATO) (The 2021 Strategy, pp. 6-7).

The 2021 Cybersecurity Strategy is based on the development of the afore-said 2011 and 2016 Strategies and, above all, on the foundations laid down for the National Cybersecurity Council (NCSR), the National Cyber Response Centre (NCAZ, Cyber-AZ) and the Central Office for Information Technology in the Security Sector (ZITiS). The implementation of the specifications and strategic objectives are carried out, in particular, by the departmental bodies of the Federal Chancellery and the ministries. Federal activities are divided between two levels of action: strategic and operational.

Ministries are responsible for the strategic orientation of their cybersecurity policy and monitoring its implementation. They are in charge of managing the activities in their remits independently, based on the principle of ministerial autonomy. At the federal level, the Federal Ministry of the Interior, Building and Community (BMI) is responsible for coordinating domestic cybersecurity policy, and the Federal Foreign Office is responsible for coordinating international cybersecurity policy. Finally, the Federal Ministry of Defence (BMVg) is responsible for cyber defence (The 2021 Strategy, p. 19).

The Strategy highlights the important role of the NCS as a coordinator that needs to bring together different perspectives from the private sector and society as a whole in the strategic advice it provides to the Federal Government. The 2016 Cybersecurity Strategy set out its specific remit as the authority competent for the identification of long-term action needs and trends, and for the development of recommendations for action. Recognising the importance of the NCSR, the current Strategy emphasises its role as the Federal Government's strategic advisory body by extending and formalising its powers. The Government expects the NCSR to provide a more comprehensive perspective on cybersecurity topics by enabling information sharing aimed at providing all stakeholders with a deeper understanding of the respective positions of those involved (The 2021 Strategy, pp. 55-56).

The operational level primarily includes the activities of the BSI as the Federal Government's central agency for information security. The BSI comprises the Federal Government, the Federal Security Operations Centre (BSOC), the Computer Emergency Response Team for federal agencies (CERT-Bund), and the National IT Situation Centre. The BSI is additionally responsible for the security and protection of the Federation's network and information technology, as well as for national critical infrastructure. The BSI is further in charge of shaping information security by providing testing, standardisation, certification, authorisation and advisory services for the government, industry and society, working closely with stakeholders from all relevant areas (The 2021 Strategy, pp. 19-20).

The Federal Office for the Protection of the Constitution (BfV) is responsible for upholding internal security, and it reports to the Federal Government and the public on security situations. It is responsible for collating and evaluating information on cyber-attacks that have extremist or terrorist motivations or that have been initiated by foreign intelligence services. The Military Counterintelligence Service (MAD) protects the Bundeswehr from espionage and sabotage as well as from extremism and terrorism in cyberspace. The Federal Intelligence Service (BND) is responsible for providing any necessary information. Gaining knowledge of other countries is relevant to the German foreign and security policy, which is included for the purpose of collating and evaluating security in cyberspace. The Bundeswehr's Cyber and Information Domain Service Headquarters (KdoCIR) coordinates cyber defence within the Bundeswehr.

In Germany, the federal states are generally responsible for the prevention of threats in cyberspace. The Federal Government has special jurisdiction over threat prevention in certain areas, such as international terrorism, security in the territory belonging to the federal railways, border protection, and national self-protection, where jurisdiction extends to the cyber domain. These tasks are carried out by the Federal Criminal Police Office (BKA), the Federal Police (BPOL) and the BSI. The judiciary is responsible for law enforcement in cyberspace, with support from state criminal police offices and police authorities, as well as from the BKA and the BPOL, as and when necessary, in line with their respective jurisdiction. The agencies listed, as well as any others involved, are coordinated at operational level in the Cyber-AZ (within the BSI structure), which serves as the central information and coordination platform.

The Central Office for Information Technology in the Security Sector (ZITiS) acts for the strengthening of cyber capabilities and digital sovereignty as a service provider for the security authorities within the remit of the Federal Ministry of the Interior, Building and Community. The federal authorities and companies that are tasked with the secure operation of federal IT infrastructure are also extremely important. They include: the Federal Agency for Public Safety Digital Radio (BDBOS), which operates the federal public safety radio networks, the Federal Information Technology Centre, and the Federal Foreign Office, as a federal operator of Germany's IT abroad. (The 2021 Strategy, p. 20).

Cooperation between the Federal Government and Länders is essential. The central authorities coordinating federal and state cooperation at a strategic level include the Standing Conference of the Interior Ministers with its cybersecurity working group at the state level, and the IT Planning Council with its information security working group. The latter is also responsible for managing information security between the federal and state governments (the 2021 Strategy, p 21). There are many forms of cooperation between the Government and Länders. First and foremost is the cooperation within CERT (VCV) or the close coordination of the state criminal police offices with the BKA as the central criminal police office. The central cybersecurity coordination offices, which are more and more often established by the federal states and linked to the BSI, are also closely involved in the cooperation at an operational level (The 2021 Strategy, p. 21).

The German Federal Government's cybersecurity policy is consistent and in line with the European Union's cybersecurity policy. Since its first Strategy adopted in 2011, Germany has consistently identified the authorities competent for cybersecurity. Efforts connected with the establishing of the National Cybersecurity Council (NCSR) and the National Cyber Response Centre in 2011, and the Central Office for Information Technology in the Security Sector (ZITiS) in 2017, as well as the participation of individual ministries in the process of building the cybersecurity system, were reprised and further clarified in the 2016 Strategy. The implementation of the NIS Directive resulted in the creation of a more transparent cybersecurity architecture. Under the IT Security Act 2.0, the BSI has been given specific competences as the national authority competent for cybersecurity. It is the Federal Office for Information Security, equipped with more and more competences, that has become the main institution for the protection of civilian cybersecurity in Germany, without prejudice to the competences of other authorities in their action area.

It is the state that plays a leading role in shaping a high level of security in cyberspace and bears the responsibility for the implementation of this policy. The state has a significant role to play and a large responsibility in ensuring a high level of cybersecurity. The state's area of activity includes the prevention, mapping, detection and counteraction of threats, incident management and criminal prosecution, counterintelligence and advanced intelligence activities conducted by the intelligence services, as well as foreign cyber policy and cyber defence. The multiplicity of tasks requires the involvement of multiple actors who, in a decentralised form, carry out tasks at both strategic and operational levels.

References:

Bendiek, A. (2016) *Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik* (Berlin: Stiftung Wissenschaft und Politik), p. 13, available at: https://www.ssoar.info/ssoar/bitstream/handle/document/46537/2016S03_bdk.pdf?sequence=1&isAllowed=y&lnkname=2016S03_bdk.pdf (July 17, 2020).

Guitton, C. (2013) Cyber insecurity as a national threat: overreaction from Germany, France and the UK?, *European Security*, 22(1), pp. 21-35.

Mickiewicz, P. (2017) System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza, *Rocznik Bezpieczeństwa Międzynarodowego*, 11(1), pp. 65-80.

Oleksiewicz, I. (2017) Polityka bezpieczeństwa cybernetycznego RFN, *Studia Bobolanum*, 28(3), pp. 41-56.

Sacewicz, K. (2021) Niemiecka strategia ochrony cyberprzestrzeni, *Przegląd Bezpieczeństwa Wewnętrznego*, 4(7), pp. 129-135.

Steller, S. (2017) Die Cyber-Sicherheitsstrategie für Deutschland, Arbeitspapiere zur Internationalen Politik und Außenpolitik, *AIPA*, 1/2017, pp. 1-84, available at: https://jaeger.uni-koeln.de/fileadmin/templates/Allgemeines/AIPA_Die_Cyber-Sicherheitsstrategie_fuer_Deutschland_Stephan_Steller.2017.pdf (July 17, 2020).

Monograph summary

The protection of fundamental rights and freedoms determines the boundaries of every regulation. At the same time, one has to bear in mind that limitations on those rights and freedoms may be dictated by the considerations of public interest, the determinant of which is public morality, among other things. It should also be noted at this point that the boundaries of general interest in the European context are determined by the purposes of public interest at the national level in Member States. Certainly, the need for such protection rather relates to specific content of public interest. Specifying that content (as far as possible) is the duty of authorities, using the instruments of national administrative bodies. The definition of regulatory purposes must take place at the national level, and the same applies to the choice of measures for fulfilling them. The instruments generally referred to in the public domain, in order to fulfil the objectives of the common good, must be subject to analysis, and to certain changes congruent with social transformations connected with technological growth, and appropriate for the specific needs of a country, its cultural, economic and political conditions, and its public morality.

The technological changes in the functioning of the digital media market or, even better, digital services, especially including the growth of the internet and social media, require a new attitude to the issues connected with ensuring the protection of the objectives of public interest. While investigating new trends in the fulfilling of the public interest in digital media, it might turn out that an entirely new regulation will be necessary. The legislator will thus be given new tasks, taking into account the premises referred to in Article 31(3) of the Constitution of the Republic of Poland (e.g., public morality, public safety, public order, and the rights and freedoms of other people).

Institute for Local Self-Government Maribor

www.lex-localis.press
info@lex-localis.press